UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, vs. DAVID TIPPENS, Defendant.	Docket No. CR16-5110RJB Tacoma, Washington October 31, 2016
UNITED STATES OF AMERICA, Plaintiff, vs. GERALD LESAN, Defendant.	Docket No. CR15-387RJB
UNITED STATES OF AMERICA, Plaintiff, vs. BRUCE LORENTE, Defendant.	Docket No. CR15-274RJB

TRANSCRIPT OF EVIDENTIARY HEARING
BEFORE THE HONORABLE ROBERT J. BRYAN
SENIOR UNITED STATES DISTRICT COURT JUDGE

Court Reporter: Teri Hendrix
Union Station Courthouse, Rm 3130
1717 Pacific Avenue
Tacoma, Washington 98402
(253) 882-3831

Proceedings recorded by mechanical stenography, transcript produced by Reporter on computer.

APPEARANCES:

For the Plaintiff:

MATTHEW HAMPTON
Assistant United States Attorney
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271

KEITH BECKER
U.S. Department of Justice
1400 New York Avenue NW, 6th Floor
Washington, DC 20530

For Defendant Tippens:

COLIN FIEMAN
Office of the Public Defender
1331 Broadway, Suite 400
Tacoma, Washington 98402

For Defendant Lesan:

ROBERT W. GOLDSMITH
Law Office of Robert W. Goldsmith
702 2nd Avenue
Seattle, Washington 98104

For Defendant Lorente:

MOHAMMAD ALI HAMOUDI
Office of the Public Defender
1601 5th Avenue, Suite 700
Seattle, Washington 98101

TABLE OF CONTENTS

October 31, 2016

TESTIMONY PAGE

BRIAN LEVINE
Direct Examination By Mr. Becker..... 13
Cross-Examination By Mr. Fieman..... 43
Redirect Examination By Mr. Becker..... 88

Monday, October 31, 2016 - 9:30 a.m.

(Defendants present.)

THE CLERK: All rise. The United States District Court is now in session, the Honorable Robert J. Bryan presiding.

THE COURT: Please be seated. Good morning. Okay. This is the time set for hearing motions in three combined cause numbers: United States versus David Tippens, Gerald Lesan and Bruce Lorente. Those are Cause Nos. 16-5110, 15-0387 and 15-0274.

I understand the defendants are all present, counsel?

MR. FIEMAN: Yes, Your Honor.

THE COURT: Their lawyers, Mr. Fieman, Mr. Goldsmith and Mr. Hamoudi, are present for the defendants.

For the government are Mr. Hampton and Mr. Becker.

MR. HAMPTON: Good morning, Your Honor.

THE COURT: There are a couple of preliminary matters. First, I wanted to find out the status of the Michaud case at this point.

MR. HAMPTON: Your Honor, the government has filed a motion to extend the briefing schedule. I don't believe that the Ninth Circuit has acted on that as yet. I haven't seen an ECF. Mr. Fieman, is that correct?

MR. FIEMAN: That's correct, Your Honor. That second request for an extension was over my objection, and we are

waiting to hear from the Ninth Circuit whether they will grant a new scheduling order.

THE COURT: Okay. In regard to Michaud, I don't know who I told, whether I told counsel or whether it was in my chambers, but it seems to me that Michaud is basically a dead issue. As long as the notice of appeal is pending, I don't have jurisdiction to do anything, and the information on the motions that are now before the Court on these cases are somewhat different, with different information, different affidavits and different briefing, as well as all the briefing that's been filed by various judges around the country on the same issues.

So it appears to me that my role is to start all over in this and take it as it comes. That's not to say that I don't have recall of what happened there, and the record of what happened there is the record.

I don't know how you propose to proceed today. There is the proposed motion -- or the motion for a pretrial conference. I delayed signing that because I anticipated that there might be a response, and there was. I have read those documents. I have not signed the order setting that up for the simple reason that I am not sure that it was necessary at this point in this case because, of course, I don't know what the government may want to show at such a hearing.

But it also crossed my mind that if it was the same

information that was presented in Michaud, there's no reason to present it again, but if there's something new that's critical to the motions here, then we can proceed with that.

MR. BECKER: Thank you, Your Honor. Your Honor, it is not the same information as was presented in Michaud. There are some critical new pieces of information, particularly the pieces of information that have triggered the filings coming under the Classified Information Procedures Act, and so we would maintain that the Court would -- we'd still maintain our request that the Court review this new material.

THE COURT: There are three motions pending here. Does that hearing have to do with one or more of those motions?

MR. BECKER: It pertains to the motion to exclude evidence because it relates to information that has not been produced to the defense that they have requested in discovery.

THE COURT: And at what point should we do that?

MR. BECKER: Your Honor, we can be prepared to present those materials today during a break. We'd need some lead time because they have to be couriered down here from the FBI, but we can make them available for Court review today. And then if the Court were to grant our motion to appoint a classified information security officer, that individual would then be responsible to contact you to provide the documents

whenever you needed to review them again and ensuring their security.

That person hasn't been appointed yet, and so today we are prepared to show Your Honor the documents. We'd have to take them back.

THE COURT: When is Barry available?

THE CLERK: He's not available 1:30 to 2:30, but he's available the rest of the day.

THE COURT: Could we set that for like 2:30?

MR. BECKER: Yes, we can do that.

THE COURT: Does that make sense?

MR. FIEMAN: Your Honor, if I may be heard briefly on that. To request clarification, my understanding from the government's pleadings is that there would be three areas that are potentially, or are in fact classified. One relates to the security risks that would arise from disclosure of the NIT code. I believe from my pleadings that that aspect of what's being submitted to the Court would be the same as in Michaud and if it's not, I would appreciate knowing that on the record.

The other two aspects -- and again, it's just my understanding -- relate to the VEP review and witness identities, and those areas would be new. Those issues were not addressed in Michaud, so if we could just clarify whether the NIT code presentation that is going to be presented,

apparently ex parte, is the same, that would be helpful.

THE COURT: Okay.

MR. BECKER: Your Honor, I am somewhat limited in what I can state in open court given the sort of issue that we are discussing. Again, as I said, there's been a change in status regarding information which led the government to make a CIPA filing, which we did not do in Michaud. So I think that's the easiest way for me to answer that question.

THE COURT: I have signed the order, and we'll plan on that at 2:30.

MR. FIEMAN: Thank you, Your Honor. I don't think I need to note my objections in the pleadings; is that correct?

THE COURT: I have your pleadings on that, that I have read.

MR. BECKER: Judge, there's one issue that I wanted to raise with respect to the defense pleadings regarding the Classified Information Procedures Act. In the defense pleading, they suggested that the government was invoking the state secrets privilege and that that would require a certification by a head of agency.

We are not invoking the state secrets privilege. That would relate to civil issues rather than criminal issues. We are operating pursuant to the Classified Information Procedures Act, and we are prepared to present additional briefing on that discreet issue which we think would be

important, if necessary.

So if the Court were going to determine that there would be some requirement of a head of agency to certify classification of data, we would ask to be able to present briefing on that issue.

THE COURT: Okay. Here's the order on that, and we'll plan on that at 2:30. That will give me an opportunity to reread the briefing you filed on it and the act itself, which I know has been in some dispute at times.

Now, we have three motions pending from all three defendants. The first, in order of filing, is docket 31 which was a Motion to Exclude Evidence. The second motion is docket 32, and that's a Motion to Dismiss Indictment. The third motion in order of filing was the Motion to Suppress Evidence in docket 35.

I have read all your pleadings at least once and mostly twice, and I don't know how you wish to proceed on these motions, in what order you want to take them or how you want to proceed on them.

MR. FIEMAN: As I understand today, the government has one witness, Your Honor. Professor Levine is here, I guess to either explain or supplement his declaration. We are not planning at this point to call any witnesses, potentially one rebuttal witness. That, of course, would all relate to the motion to exclude.

The defense believes that all of the facts and evidence that the Court needs to decide the motion to suppress and also the *Franks* motion folded in there, as well as the motion to exclude, is already all before the Court in terms of the exhibits and declarations that have been submitted.

So that would leave just one witness, is my understanding, from the government on the motion to exclude and discovery issues.

THE COURT: Are you all suggesting we take the motion to exclude first?

MR. FIEMAN: Your Honor, what I would anticipate as maybe being workable is for them to offer their witness, take the testimony on that and then, subject to your review of the classified records, we would then be prepared to argue all of the issues in one argument together.

THE COURT: Mr. Becker, Mr. Hampton?

MR. BECKER: Your Honor, we think that's workable.

THE COURT: Okay.

MR. GOLDSMITH: Could I just add one thing, just for the record? On behalf of all three defendants, any time Mr. Fieman speaks, we are joining into all of his objections and arguments, just so that the record is clear, Your Honor.

THE COURT: I understand.

MR. HAMOUDI: Thank you, Your Honor.

THE COURT: Now, on this motion to exclude, my law

clerk pointed out to me that he wasn't sure here in the record that in these cases a specific discovery request has been made, that the government has not responded to, that responds to this motion.

MR. FIEMAN: If I may clarify, Your Honor. Certainly what we noted in our initial motion to exclude pleading was that we had made a request to the government for disclosure of all the NIT components, most clearly laid out in Vlad Tsyrklevich's declaration which was submitted as an exhibit to our motion to exclude docket 31 and --

THE COURT: You think that preliminary matter is part of the record?

MR. FIEMAN: Yes, Your Honor. And my understanding is that the government has declined, as in Michaud, to provide that discovery, with one development noted in our pleading from last Wednesday. Apparently, we will be getting some or all codes related to the identifiers now.

MR. HAMPTON: Your Honor, as to the unique identifiers code, we have provided that, so that has been provided. We have also provided, as we have, and are willing to make available the pay load component. I think that's understood, but just to make sure we are clear on that as well.

MR. FIEMAN: Well, if I can make sure the record is clear. The payload component that was provided is the one

that is referenced in Mr. Tsyrklevich's declaration. We have not received any additional code.

Our understanding -- again based on that declaration and some other information that we will develop through Professor Levine -- that was a partial payload or partial code, so we are contending there's still a complete payload that's missing, but they did provide some payload code just -- nothing has been provided since the Michaud ruling except the identifier issue.

THE COURT: Now, does either side wish to make any opening comments before we hear testimony?

MR. HAMPTON: Your Honor, I apologize. I want to confirm one thing. We do disagree with that assessment. I realize that's a matter for the Court, and we will resolve that, but we believe we have provided or are willing to make available the full payload.

I neglected to mention that we also made available the network packet traces for each of the three defendants' interactions with the FBI. So the defense has thus far declined to examine those, but they are available, and I just want that on the record.

THE COURT: Do you wish to make any other comments before we start?

MR. FIEMAN: No, thank you, Your Honor. I think that clarifies the record where we disagree about it.

THE COURT: All right. You may call your witness.

MR. BECKER: At this time, the government calls Brian Levine.

THE COURT: If you'll raise your right hand and be sworn.

BRIAN LEVINE, called as a witness, duly sworn.

THE COURT: Please be seated. Let me ask you to speak right into the mike and keep your voice up, please.

MR. BECKER: Your Honor, if I can just have a brief moment to set the computer up. Could I ask the Court staff, we are not publishing the computer now.

THE CLERK: You wanted it unpublished?

MR. BECKER: Yes. Thank you.

THE COURT: Okay.

BY MR. BECKER: May I inquire, Your Honor?

DIRECT EXAMINATION

BY MR. BECKER:

Q. Sir, can you start by stating and spelling your full name for the record?

A. My name is Brian Levine, B-r-i-a-n L-e-v-i-n-e.

Q. What do you do for a living?

A. I am currently a professor in the College of Information and Computer Sciences at the University of Massachusetts, Amherst. I joined the faculty in 1999 as an assistant professor. I was granted tenure in 2005. I was promoted to

professor -- full professor, as they say, in 2010 and I have continued there. I am also the director of the Cyber Security Institute at UMass, Amherst, and I have various functions as a professor there.

Q. So for how long in total have you been working as a professor at UMass, Amherst?

A. Since 1999.

THE COURT: Counsel, I have read his CV and his report.

MR. BECKER: Your Honor, we'll just briefly go through his credentials.

BY MR. BECKER:

Q. What do your current duties include?

A. As a professor as UMass, Amherst, my duties include research. My research typically involves undergrads, but more often graduate students seeking a Master's or Ph.D. degree. That research, as a brief summary, relates to digital forensics, forensic investigation, crimes against children on the internet, networks, network security and so on, as detailed in the declaration that I submitted.

In terms of teaching, I teach a variety of classes also listed in the declaration, including digital forensics, computer networks, security at the graduate and undergraduate level and so on. As a service component of my job, I often lead conferences where we -- and workshops -- where we review

papers submitted for review by peers. I'm one of the peers, so to speak.
Q. Have you personally been published in peer review journals and similar publications?
A. Yes. Since the time I started as a graduate student, I started publishing in peer review conferences and their relative venues, and I published something like 80 peer reviewed papers on the topics that I mentioned.
Q. Other than your work as a professor, what other sort of employment have you had in your field?
A. Both as a -- during my time as a graduate student and after graduation, I worked at various places, and also during a year-long sabbatical, so I worked at what's called Bell Labs -- it used to be owned by Lucent when I worked there -- Intel research labs, Sprint research labs. I spent a year at a local company in Massachusetts working on Internet advertising, for example.
Q. Can you describe your educational background?
A. I received my bachelor's of science in applied math and computer science from the University of Albany. From there, I went to graduate school and received a master's and Ph.D. in computer engineering. My dissertation focused on the internet and how groups of people can use the internet to communicate.
Q. How are you able to keep your skills and knowledge current?

A. Well, teaching. Certainly, the classes I teach I always maintain the material to be current with state of the art, but certainly working on research papers, my goal is to advance that state-of-the-art and in writing those papers I have to reference, of course, related work.

And as I mentioned before, leading peer review panels or even serving on peer review panels keeps me informed on the latest work, even perhaps prior to its publication.

Q. Have you specifically been involved in researching work related to child pornography dissemination over the internet?

A. Yes. I have a number of publications that relate to that and various aspects of it. Since 2008, I have been funded by various agencies in the United States government to work on these topics. I was first -- I first responded to a public solicitation from the National Institute of Justice to work on novel methods and tools that can be deployed across the nation to investigate Internet-based crimes against children.

From there, I received funding from various agencies, including the National Science Foundation. Currently, I am funded by the Federal Bureau of Investigation to research and deploy tools on these types of crimes.

Q. Now, to be clear, did you have any involvement in the investigation of the Playpen website?

A. Not at all. I was not involved. Our tools were not used. I was not involved in that operation.

Q. Did you have any involvement in the development or deployment of any network investigative technique related to the Playpen website?
A. Not at all.
Q. Are you being paid for your time in connection with preparing your declaration and your testimony today?
A. Yes, I am being paid by the U.S. Attorney's Office for my time today.
Q. Has any of this work been done pursuant to any contract you have with the FBI?
A. Not at all.
Q. Professor Levine, I want to ask you if you can describe for the Court, before you prepared your declaration in preparation for your testimony, what documents and information did you review?
A. So this is also summarized in my declaration, but there is one addition since then, but to briefly summarize what's already in there, I reviewed the expert declarations of the defense team, including Mr. Tsyrklevich, Mr. Young, Professor Miller, Professor Reyzin and Mr. Kasal.
I have also read Special Agent Alfin's affidavit -- or declaration, I should say; various documents related to evidence that was collected that I list more specifically in the declaration I submitted. I also looked at the payload components that were provided to me. I looked at the traces

specific to each of the three cases. I should clarify there are three payloads as well, one for each case.

I looked at data from the FBI about what was recorded by them as these three cases proceeded. And since my declaration, I was provided with the source code for what the FBI used to generate the identifiers.

Q. Is it your understanding that all of the information you were provided for review was also made available to the defense team?

A. That's my understanding, including the source code that I mentioned.

Q. Did you review any related exploit or government server information?

A. I did not.

Q. Professor Levine, I want to ask you next about some basics of internet communications. First of all, would it assist you in your testimony to use a demonstrative exhibit?

A. Yes, it would.

Q. Have you --

MR. BECKER: First of all, Your Honor, if I can approach, I do have a hard copy of that, and we are also going to present it using the computer.

For the record, we have marked this as demonstrative Government's Exhibit No. 1.

BY MR. BECKER:

Q. Professor Levine, do you recognize -- just take a look through the paper. Do you recognize Government Exhibit 1?
A. I do.
Q. Is that the demonstrative exhibit that you prepared?
A. Yes, it is.
Q. Have you also reviewed a digital copy of that on the laptop in front of you?
A. Yes.
Q. Are they substantially the same?
A. Yes.
MR. BECKER: Permission to publish using the electronic version?
MR. FIEMAN: I have seen all their exhibits. We have no objection to any of them.
THE COURT: Okay. The exhibit may be admitted for illustrative purposes and may be published.
BY MR. BECKER:
Q. Okay. Professor Levine, do you have the first slide on the monitor in front of you?
A. I do.
Q. Can you just start by explaining -- at a basic level -- a sort of ordinary or standard internet communication between a user and website?
A. What the slide shows is something that I believe many people experience every day, and that's starting from the

laptop on the left, their own laptop, they would like to contact some internet website. Some examples are presented on the right side of the slide, for example, Google or Amazon. Many other websites of course exist.

So to do that, there's going to be a series of internet protocols that are involved, that ensure that that information gets to its destination, and that process has a useful analogy to the postal system.

So if you were to advance one slide. Thank you. So now you can seek this green line that's going from the internet user to the website. Any particular user will want to contact this website and receive information back. So how does that work? There are three protocols involved, and they correspond to this postal system analogy.

There will be an envelope that carries a "to" address and a "from" address. The IP protocol handles that. Similarly, the mail carrier or the mail system can't deliver a message unless the destination is specified correctly, and you can't receive a message back from your pen pal to form a communication back and forth unless you included a from address or a source address, as it's called on the internet, on the outside of the envelope.

At another level, there will be an analogy to certified mail. There's a protocol in the internet called TCP, or transmission control protocol, and it provides what's called a

reliable service to deliver information across the network, and that's again very much like certified mail.

Among the things that TCP does is check to make sure that the data maintained its integrity as it traveled across the internet. It numbers the information as it goes across the internet such that the other side can confirm that everything that was numbered was received indeed. A request can be made by the other side to resend information that is missing due to this numbering, and anything that is received out of order can be reordered by the other side.

Additionally, at the start of TCP, there's a hand shake where one says, are you ready to start communicating, the other side says yes, I am ready to start, and then the other side says yes, let's get going.

So then at the end, when all communications are done, each side can say good-bye and say in fact everything that was sent I received, I am all done, I don't need any other transmissions. So this -- I can't tell you how many times this happens across the internet per day. It must be millions or billions, a very common protocol.

So then there's the content of the message, which is this HTTP request or web request, and that might be analogous to a request from a merchant to purchase something. Here what we are saying is, I would like this website that you provided, and the response will be, here's the website, and that can get

more detailed as the website is larger and so on.

So that's standard. The most important thing to note in our context is that when the communication is open, it's sent reliably. The fact that there's an address, not only a destination address but a source address, and the communication goes back and forth, there's the type of communication that that's the person you are talking to.

Of course, it reveals the IP address, the public addresses that are assigned to both sides, and information is again provided reliably. So that's standard, what you might call typical communications on the internet.

Q. If I can move you to a second slide. Can you illustrate how communications via the Tor network might differ?

A. So as I said at the previous slide, at the end of any typical communication using TCP, of course you reveal your IP address to the other side. So Tor was designed to not reveal to the website the IP address of the Tor user -- if you wouldn't mind advancing one more -- and Tor, as represented on the slide, is a collection of volunteers who have put up computers on the internet that accept traffic.

Here, I put up a sample, nine of them, but the numbers are in the many of thousands, and instead of directly communicating with the website using the standard means I described earlier, the Tor user will relay the information through a series of proxies. So without getting into the

extraordinary number of details at the highest level, the Tor user will pick some random three -- and then if you don't mind advancing once more -- and then form a connection to the first one, form a connection to the second one, form a connection to the third one.

And again, I am eliminating some details, but essentially this is an encrypted connection, and then you can see there's a red arrow out of the last relay. So some important details are that that first relay on the left side of the screen knows the IP address of the Tor user, which is what we are trying to hide from the website. The last relay notes the website's IP address but, due to the mechanisms in Tor, it does not know the IP address of the Tor user.

That last relay on the right side of the screen also does not know the IP address of the first relay because they are not directly connected; there's someone in between. The last relay does know -- in cases where the connection is non-encrypted -- the contents that the Tor user has sent to the internet website. There would have to be some other mechanism in place to secure that content.

So if you connect to Amazon securely over Tor, HTTPS, your browser lock turns a different color maybe, then that last Tor relay would not know the contents. But if the connection is just a plain text connection, that last Tor relay would. So one limitation here, of course, is that the Tor user knows the

IP address of Amazon, knows the IP address of Google, these web addresses that were provided, and that may not be sufficient in some cases.

Q. That's because in this scenario, in this slide, we are looking at a Tor user who's accessing a regular website off the internet?

A. That's right. It's not a website that's seeking any kind of anonymity themselves, they are just allowing people to connect to them through Tor.

Q. If we can move to the next slide, and can you describe how access to a Tor hidden service differs at all in this process?

A. Yes, it differs in a number of important details. First of all, in a Tor hidden service -- again, it's the website, for example -- it's the website that would like to maintain its IP address as something that it would not like to reveal to people that visited. So we are going to need a little bit more machinery, and there's a few steps involved.

So the first step is that hidden service, which is really just a web server in this case. It finds three or selects at random three volunteer relays from the Tor network and, like before, forms a connection out. I am going to skip some of the real details of Tor here in order to present the high level.

But once that's created -- if you don't mind advancing once more -- they will release a document or a file, which I

will just call an onion file, to the world, and so that doesn't necessarily go out over the Tor network. They might email that to their friends. They might announce it in a chat room. Whatever it is, they announce to the world this onion file.

A Tor user will somehow come in contact with the onion file, and that's important because that onion file contains a secret, and it's a secret about forming an encrypted connection to the hidden service. So with that secret, with that key in place effectively, the Tor user will then create, as before, their own circuit through the seven volunteer Tor relays -- if you don't mind advancing -- again, picking three, and those three bridge together with the original three, and now we have a connection through this Tor network inside the cloud in the diagram.

Now, unlike before, we have the advantage that because of the onion file, no one in the middle actually gets to see the plain text, even if that Tor user connects to the hidden service through a standard, unencrypted, plain view protocol. We do have what we had before, the left most relay closest to the Tor user knows its IP address, the right most relay in the diagram knows the IP address of the hidden service, but they don't know each other. If they tamper with the traffic, then the encryption that's used end-to-end would detect that and the packets would be dropped. So I think that summarizes

everything.
Q. Next I want to ask you if you can describe how the process of the network investigative technique would work in this sort of network setup.
A. So the network investigative technique obviously is relevant to these cases, and the problem, of course, that it's trying to solve is that from the hidden service's point of view, the IP address of the Tor user is not revealed. So the network investigative technique, as described and available to me in the documents that I have read, works as follows: The FBI will put up a server and then we know -- we all know that the FBI seizes control of the hidden service -- if you don't mind advancing -- and at that point, they will place the NIT as part of the hidden service such that our Tor user who creates a connection using that onion file, all the way through the Tor network as it appears on the slide, will make connection to the Tor hidden service, log in, request a page from the hidden service, and the Tor hidden service will return to them the payload, and the exploit will travel through the Tor network and arrive at the Tor user.
I should say -- I should go back. After the NIT is available on the hidden service but before the Tor -- before the Tor user requests the page, the hidden service -- which is again seized by the FBI -- coordinates with the server to generate and obtain this unique ID. That unique ID is placed

in the NIT. It's tailored to this particular visitor and when the NIT is returned to the Tor user, the exploit is a method of access by which the payload can be executed.

The payload acquires information from the Tor user -- if you don't mind advancing. That information, which is really -- the ID is really what we are mostly concerned with here -- would be returned outside of Tor. So because it's returned outside of Tor, that ID can be associated with the IP address that appears in the packet sent from that Tor user.

So we have a full circle. We have the hidden service, it's waiting for Tor users to come. Each user, there's an ID that's generated, that's embedded in the NIT, the NIT is delivered through the Tor network. The exploit is a method of access that allows the payload to run. The payload sends the message, which is that unique identifier, most importantly, and that's received by the FBI server.

The FBI server can confirm that that is indeed a unique ID that is generated. And then we are really back to the standard set of techniques with an IP address. For example, an investigator could subpoena information from an IP -- about the billing address for that particular IP address, and things proceed as is more typical with investigators.

Q. So why is it that the IP address that's returned is actually visible to the server that receives it?

A. So that arrow information sent outside of Tor on the left

of the diagram is a standard IP based, TCP based, HTTP request that I started with in the very first slide. The standard connection -- it's that analogy of sending mail through the post office. There's a return address, in our case a source address, that the FBI server receives.

And again, the FBI server doesn't receive just one message. It's a TCP connection with our hand shake, with the number of packets, recovery from loss, recovery from out of work delivery and then a good-bye. So not only that TCP provides, as I mentioned before, check zones that ensure the integrity of information that goes past it, and the information itself is exactly the number that the FBI generated prior to the NIT being delivered to the Tor user, and as I might explain later, the number is so large that it's difficult for someone to guess a value that the FBI might have generated.

Q. All right. I want to ask you about some components of this system that you've reviewed, so let's move to that. We can start with what you have described as the payload.

What did you review with respect to the payload? What did that consist of?

A. So the three payload files that I was given, one corresponded to each case. Each payload had a corresponding packet trace or PCAP file, as it's sometimes called in some of the declarations.

Each payload had an embedded identifier just like the one I described earlier. The files had various differences, but for example, one of them had a code in it that was easily human-readable. Some code is meant for a computer, other code is what's called a script. It's very easily readable if you have the training, and I was able to look at that human-readable code and execute each instruction.

These instructions gathered exactly what was described in the warrant application that I reviewed. For instance, the operating system version, and I could see that the same information was available in the packet traces itself.

Q. Did you notice anything abnormal from the review of those instructions and the packet traces?

A. Right. So the packet traces are -- there's three of them, one for each case. Each was a little bit different because of the variations of -- it was a live internet trace, but they all conformed to exactly the general summary that I gave before.

For each one, I could see that there was a TCP request for a connection, the other side of the hand shake, the third hand shake and then I could see the web request go out. Very cleanly and very visible, without any expertise, you could see in the outgoing packet that the unique ID was present. There's other information that's in my declaration that I alluded to, but for instance, all three cases shared a common

random number, a case ID.

When available, other information was also recorded in this packet that went out, that looked like a web request, including as I say the operating system or host name or other information. The FBI server responds with oh, I am sorry that web page is not available, and then the connection is essentially closed after tidying up any missing packets out of order or things like that.

I was also able to, by looking at these individual packet traces, confirm that these integrity checks that I mentioned, these check zones, were valid. There's in fact two check zones on each of the packets going out -- and when I say going out, I mean going out from the defendants' computers -- I could see that they were valid, they were fine.

There was also no indication of various attacks that might have taken place, extra packets, odd occurrences. They looked very straightforward. They appeared to do exactly what was described in the warrant and conform to, for instance, what I saw in the payload.

Q. Now, were the ingredients there, so to speak, in order for someone to do further testing of that payload information?

A. Yeah, in fact all told, that's a lot of information. So for example, I know -- I didn't personally examine them, but I know that what are called the images, the record of the defendants' computers as they were seized, is available. So

those were the computers that these payloads were executed on.
The payloads are also available for executing on other computers. The output of -- in other words, the output of the payload, which is the packet capture, is in a standard format that's easily viewable by anyone who knows these techniques. If the goal is to verify that indeed this ID appeared in the packet trace, they were there. If the goal is to verify that the information that is in the packet traces conforms to the warrant, those ingredients are there. If the goal is to figure out what else this payload might have done, they can be run -- they can be run on other computers.
Q. Now, one of the requests in this case, as you are aware, is for disclosure of the exploit component. Would it be necessary to have the exploit in order to run the sort of testing that you've been talking about?
A. No, because the exploit is a method of access. It's equivalent or analogous, rather, to a lock picking device. So if the goal is to determine whether that identifier appeared in the payload, the exploit is not necessary for that. All I need to do is look at -- if I said -- let me restate my response.
If the goal is to validate or verify that the ID is present in the packet traces, one need only look at the packet traces. If the goal is to examine what this payload did, one can look at the payload. The method of access to deliver the

payload is not the same as the payload itself.
Q. Now, what if you wanted to determine whether this TCP connection was subject to some kind of attack, are the ingredients there for that?
A. So the ingredients are there. The packet trace itself is extremely explicit. It's low level. It's not just a printout of the web request. It's the actual TCP packet at the lowest level. Reviewing the exploit would not add information to examining that packet trace. As I said before, the packet trace includes the integrity checks, the call sequence numbers, all the recovery mechanisms, it's all there.
Q. Professor, did you also review the code used to generate unique identifiers?
A. Yes. In fact, this code is very short. It's exactly one line, because it leverages an industry standard technique. It uses an industry standard library. It's called UI. It uses version 4 of UUID, which has the computer it runs on generate a very -- well, pick from among a very large space of random numbers. It's used extremely widely. It's used all over the internet by Google for its advertisements. It's widely used. That code is easy to review.
I looked at the underlying library as well. It's the industry standard. In my declaration, I did not have access to that code when I stated it, but with the exception of a small detail, it conforms exactly to what I stated in my

declaration in terms of its ability to generate numbers that are unique without duplication.
Q. Did you notice anything abnormal about that code?
A. No, it's exactly one line. It's entirely appropriate. It's very simple. There is not much to examine.
Q. Using that particular type of code, what would be the general probability of there being duplicates?
A. Nil. The exact numbers are in my declaration. It's astronomically low. Even so, it's trivial to detect those duplicates.
Q. What do you mean by that, that it's trivial to detect them?
A. Well, if one had a list of all ID's that were generated during this operation, one need only find duplicates that are there. There's no algorithm. There's no exercise to be done. There is no trick. You could load them into an Excel spreadsheet and ask them to detect them. There's nothing to do.
Q. What is your understanding of whether that review was done with respect to this investigation?
A. As I stated in my declaration -- well, more specifically you can look at Special Agent Dan Alfin's declaration, and he notes that he fact checked for those duplicates. As I stated, I find it hard to believe that that was not a trivial task, but I am sure he got that right. There's nothing to do.

Q. Would review of the exploit be necessary to make any of those determinations about the unique identifiers?
A. The exploit is a completely separate piece of code. That is not run on the server. It's not related to this unique ID. Selecting the entire code is available in this one line. It's not related to the exploit.
Q. Let's move more specifically to that concept then. I want to ask you first, Professor Levine, if you could just start by defining a term for us. Could you define the term malware? What is malware?
A. So malware is code that through some method of access executes on someone's machine, generally for some task that is deemed malicious, hence the MAL in malware.
Q. What are the components of malware?
A. The components are apparent from my definition, actually. There's a method of access, and then there's an activity that happens. I think that at a high level that describes all malware. So for example, what I mean by a method of access is some malware -- some malware is -- the method of access is what some people call phishing or social engineering or good old-fashioned trickery. You might get an email that appears to be from a friend, and they ask you to run the attached code, and that attached code does something.
Another method of access is, you might be given a USB key from a coworker, you might find a USB on the floor at a cafe,

plug that USB key into your computer, that is the method of access. The code that runs, that was stored on that USB code, could do anything.

A third might be advanced code that's written by someone to circumvent protections on your computer that were normally provided by the operating system. That would be a method of access. The separate component would be the task, what does it actually do?

Q. So how does that method of access differ from the actual, what it does, the malicious activity?

A. It differs quite a bit. So the activity that it does, I might tell you that malware on my machine sent spam, unbeknownst to me, to different people. I might tell you that it recorded my key strokes so that my banking credentials could be stolen. It might be that materials were stored on my computer unbeknownst to me. But that's a different thing.

Perhaps one analogy that explains that is, if I tell you that my house was broken into, you might say how did they get in? And I might say, they got in through the door or I might say they got in through the garage or the basement. The next question has to be, what did they do when they got inside? How they got in doesn't tell you what they did.

Then I might say oh, when they got in, they stole cash from my safe. They left materials in my garage. They did other things. In fact, if I had started with, there was a

break-in at my house and they stole cash from my safe, your next question has to be, how did they get in? These are two separated concepts. Knowing one is not sufficient to know the other.

So the same is true in malware. If I tell you that I received what's called a trojan horse, which means that I downloaded a program that appeared to be a tick-tack-toe game but in fact what it really did is run some other activity, your next question has to be what did the trojan horse deliver? And then I might say, it was a key stroke logger or I might say it stored files on my computer. But knowing how that malware got on my machine, the method of access, is not the same as what it did.

Q. So how does that line up with the scenario that we are talking about here regarding the deployment of the NIT?

A. So as I stated before, that exploit has this function of a method of access, and the payload is the activity that was done. So in these cases, knowing the method of access would be observable or notable from looking at the exploit. But on the other hand, the payload tells you what was done once access was gained.

Q. So the defendants have suggested that it is possible that someone else could have used, say, the same method of access, the same exploit to, for example, plant child pornography on their computers.

First, in a general, theoretical sense, is that possible?
A. Yes.
Q. Would examining the exploit that was used in connection with these cases support or refute that theory?
A. It would not support or refute that theory because, like the analogy I gave before, knowing that a computer is -- knowing that a method of access is available on a particular computer does not tell you what else was done. So, for example, if I was to examine that exploit, perhaps one of two things would happen.

The first thing might be that in examining the exploit, I might discover that first, in executing and allowing this method of access, it leaves a trace on the computer. The other might be that it leaves no trace.

Well, actually in the second case, if the exploit leaves no trace whatsoever, examining the exploit does nothing for me because I have no information to act on to look for other software or malware that might use the same method of access. So let's go back to that first case.

In examining the exploit, let's say that I hypothetically discover that it does leave a trace on the computer, some type of artifact that indicates that that was the method of access. Having that actually still does not support or refute other theories that I have about how this computer might have been used by some other malware with the same method of access.

Like the house analogy, hearing that someone can get in through my windows doesn't say what they are going to do when they get there. Examining the exploit, discovering that there is information that can be gained from it or not, but whether there is information that can be gained from it does not tell me whether later, even if I find that same trace, what that other software did.

This is not a property of malware. It's just a property of software; the same functions of software can appear in other software. What it does after that function is run -- in the case of malware, certainly -- is anything that that computer can do. If the computer has a CPU, it can compute. If the computer has storage, it can store files. If it's connected to a network, it can send things over the internet.

Q. In a scenario where we are talking about malware that was designed to download and store child pornography, would it necessarily depend on any one particular method of access to be possible?

A. Absolutely not. A method of access is just the first stage -- it's just one component of malware that can do anything after it. So telling me that a computer was vulnerable to a trojan horse, again my next question has to be what happened next? If you started with the malicious effects of that software, my first question would then be, how did it get in? They are unrelated.

Q. In terms of looking for malware itself on your machine, where would you look in order to make those sorts of determinations about codes that ran and what it could have done?
A. So if you are looking for malware, for instance what you are really looking for is what did it do to your computer. So you would look for evidence of those activities. So for instance, if it's malware that sent spam, you would look for a code that has aspects of it that related to an email. If you are looking for malware that is related to storing images on a computer, you would look for evidence of that type of activity in the program.

On the other hand, you could look for malware based upon this method of access. So you could look at whether files that are core to the operating system have been changed. Operating systems, because they are public, the files that run them, the engine of the operating systems are well-known and any changes in them can be easily detected.

There's a long list of things that could happen. For example, some malware actually prevents a computer from being upgraded. You could tell whether the computer prevents that. You could test whether files have different time stamps on them. You can test whether they have their permissions changed.

Windows computers, for example, have a very important

component called the registry. It's a massive catalog of permissions and access controls and configurations, and there's a long list of standard entries in this registry that can be looked at to look for evidence of malware.

There's many other components. File systems, the malware can hide in the first sectors of the file system, the last sectors, in the middle. I teach an entire course on digital forensics, and we spend at least a semester going through all the different places that you can examine a computer for use by somebody as part of an incident.

Q. So the defense has suggested that it's possible that an exploit could have, for example, altered security settings on the defendants' computers.

First, as a theoretical premise, is that possible?

A. Yes.

Q. Would you need to review the method of access to determine what the computer's security settings are?

A. No. In fact, every owner of a computer should look at their computer and look at the security settings and see whether they allow for some unexpected access. Those same settings can be evaluated after an event happens. It's one of the first -- or maybe not the first, but it's definitely a very critical step of recovering from some event is to then go back and examine those settings. So anyone trained in a variety of related tasks, such as securing a computer,

recovering from an incident, investigating an incident, has a list of activities, places, things they can do to examine a machine.
Q. You mentioned that you reviewed the defense expert's declarations. Did you see any indication of a review or a finding of changed or altered security settings or a particular vulnerability?
A. I didn't see any in the declarations that I reviewed before I wrote my own declaration, and in the response to my declaration, I didn't see a note of any of those findings. There was a note in that response about Mr. Young examining the computer. I didn't see it in that declaration, a statement to that. So not to my knowledge.
Q. So, Professor Levine, to kind of bring this to a conclusion here --
MR. BECKER: Your Honor, if I could have the Court's indulgence for just a quick moment, if I could have a brief moment.
THE COURT: Sure.
(Off the record discussion.)
BY MR. BECKER:
Q. Professor Levine, to sort of bring us to a conclusion, would reviewing the exploit, the method of access, help to find malicious software or malware related to child pornography?

A. No, because as I have said, knowing the method of access does not give you information about malware that might have run subsequent to that, whether the malware used the same method of access or a different method of access.

Q. Would reviewing the exploit, the method of access, help determine whether the payload was delivered accurately to the defendants' computers?

A. No, because in this case, the payload was delivered by the Tor network. As I explained earlier, that connection is encrypted for every volunteer router along the way, and the exploit is not involved in it.

Q. Would reviewing the exploit help determine what commands the payload executed or what it collected?

A. No. In fact, the payload is the best place to look to see what commands the payload executed.

Q. Would reviewing the exploit or method of access help determine whether the payload data was delivered back securely?

A. No. In fact, the packet traces are PCAP files, which are available, are the place to look to see whether that information was returned accurately. Additionally, that information is returned on systems that didn't see the exploit, so it's not relevant.

Q. Would reviewing the exploit help determine whether the unique identifiers were chosen reliably?

A. No. In fact, we have the source codes for how those identifiers were chosen, and it doesn't involve the exploit.

MR. BECKER: Your Honor, those are all the questions that I have for Professor Levine, unless Your Honor has specific questions.

MR. FIEMAN: Your Honor, may we have a five-minute recess so I can change out my computer?

THE COURT: That's fine. Let me know when you are ready.

MR. FIEMAN: Thank you, Your Honor.

(Morning recess.)

THE COURT: Be seated, please.

Mr. Fieman.

MR. FIEMAN: Thank you, Your Honor.

CROSS-EXAMINATION

BY MR. FIEMAN:

Q. Good morning, Professor Levine. We just introduced ourselves over the break, but for the record, my name is Colin Fieman. I represent Mr. Tippens in these proceedings.

A. Good morning.

Q. I have a fair amount of ground to cover, and I am not a technical person, so please, if I ask something that's confusing or I just don't have it right, feel free to clarify.

A. Okay.

Q. Now, I just want to start -- what I am hoping is we are

actually going to find areas more where you agree with our experts than disagree, which I think you summarized in your declaration today. So I am going to try to focus on the areas where we overlap.

In order to do that, I would like to just get some basic terminology or principles clear.

THE COURT: This isn't working.

BY MR. FIEMAN:

Q. So Professor Levine, let me start, just as a basic principle, you agree that collecting reliable and accurate digital evidence in internet cases can be challenging? It's not like your typical drug case or something where you actually have physical drugs to analyze?

A. Well, I don't have experience with drug cases, but in general, forensics is a difficult problem.

Q. It is. And you have, in fact, written about some of those challenges, I think, in your work. I had the opportunity over the weekend to try to read your Efficient Tagging of Remote Peers article. Is that an article that you presented with some cowriters?

A. Yes. Do you have the article here so I can verify what we are talking about?

MR. FIEMAN: If I may approach, Your Honor. We'd like to have this marked as Exhibit 1. There should be a bench copy as well. It's an article from Professor Levine,

and copies have also been provided to the prosecution.
A. Yes, this appears to be the article I have written.
BY MR. FIEMAN:
Q. Is this an accurate quotation from your article -- I think there's a typo in there, because I did capture it from the original -- but as a basic principle, "strengthening techniques used in network-based criminal investigations" -- and some of those concerns have been addressed by, for example, the National Academy of Sciences, calling for a scientific overhaul?
A. So I am sorry. Are you asking me to confirm that this is in my article, or are you asking me to confirm the statement? What exactly are you asking?
Q. Are you confirming that's a correct statement of what the National Academy of Sciences is calling for?
A. Yes. The reference in -- the article referenced that report which came out a number of years ago talking about forensics, broadly ballistics, digital evidence and so on.
Q. Correct. I am going to narrow as we go. I think there's a typo. I think it says "investigations beings"; it should be "investigations begins"?
A. I apologize. There was no copy editor for these documents. It's just me.
Q. I hope you review your code a little more carefully. Did you have a chance to proofread that article?

A. Did I have a chance to proofread this?
Q. Yes.
A. Yes, I tried, certainly.
Q. Now, is it fair to say that one way to ensure that digital evidence, forensic evidence in a particular case, is accurate and reliable for a jury is to have qualified experts review it for possible errors?
A. The evidence that was collected?
Q. Any evidence. Before evidence -- digital evidence is presented to a jury, is it fair to say that one way to ensure that it's reliable and accurate is for qualified experts to review it?
A. Yes. I assume you are talking about digital evidence that was, for instance, seized from the scene?
Q. Correct.
A. Yes.
Q. Now, one area of expertise that I understand you have is with peer-to-peer networks or P2P networks; is that correct?
A. That's correct.
Q. Are you familiar with a software or program called EP2P?
A. I am not very familiar with it. EP2P is a program that I honestly just know its name. I was not involved in its construction design. I have never seen it, never held it, never seen it demonstrated, so I don't know much about it at all.

Q. So you haven't had a chance, for example, to review EP2P software?
A. No.
Q. So you are not in a position to comment on it; is that correct?
A. Well, it depends on what your question is, but no.
Q. Now, would you agree just as a general matter, not based on any specific knowledge, that if a defendant was charged with file sharing via a P2P network or over a P2P program, his computer expert should be able to analyze that software to make sure it was identified correctly? Do you agree with that as a general statement of principle?
MR. BECKER: Objection to relevance.
THE COURT: He can answer.
A. I am sorry, can you repeat the question?
BY MR. FIEMAN:
Q. Just as a general matter, focussing on P2P networks, because that's something you are particularly familiar with, would it be a fair statement that if a defendant was charged in a criminal case based upon identifying information collected on a P2P network, that his expert should be able to analyze and check the software that was used to collect that information?
A. If you are asking my opinion on a legal matter --
Q. No, just as a general matter of principle. If you are

doing work as an expert, is that a fair statement?
A. What principle? Sure, I don't know what principle you are referring to. In general fairness or a legal principle or...?
Q. As general fairness and to ensure accuracy...
A. Accuracy of the evidence collected over the P2P network?
Q. Yes.
A. For instance, they could look at the evidence itself. One of the ways in which you might provide that fairness is to look at the tool that was used; it might not be the only way.
Q. Okay. What about looking at the P2P software itself?
A. Which P2P software? The one used by the client or the one used by the investigator?
Q. The one used by law enforcement.
A. That, in addition to other methods, would be one way.
Q. Now, Professor Levine, I understand that the word NIT or Network Investigative Technique really covers could relate to a lot of different stuff, but have you ever worked on a case involving a NIT?
A. So why don't you define NIT, because I believe -- because you are describing it so broadly, I am not sure what you are referring to. My understanding of a NIT is that it refers to the techniques used in this case as I described in my earlier statements, and in that sense, this is the only case that I have worked on that involves a NIT.
Q. Okay. Are you familiar with a prior FBI operation called

Operation Torpedo?
A. Only from reading about it in the news.
Q. Okay. Are you aware that defense experts, Professor Miller and Shawn Kasal, actually worked on the Operation Torpedo case?
A. Only as described in their declarations.
Q. And you are aware also, from Robert Young's declaration which you say that you reviewed, that he's an expert in forensic analysis, digital analysis?
A. I am aware that he wrote that, yes.
Q. Have you ever been qualified in a court or any judicial proceeding as an expert in forensic evidentiary analysis?
A. Not in a court proceeding, no.
Q. You say that some of your research is currently funded by the FBI; is that correct?
A. Yes.
Q. How much funding are you receiving and over what number of years or terms?
A. The current contract is for -- this is from memory, but I believe these are correct. The current contract is for $400,000. It's over a 12-month period. That $400,000, for example, covers what's called the overhead of the university, a variety of costs and so on. Does that answer your question sufficiently?
Q. It does. Thank you, professor.

Now, I just want to be clear on what you have looked at in connection with this case in terms of code or components and what you have not had the opportunity to look at. So I just want to clarify that.
A. Okay.
Q. Now, have you in fact looked at the exploit component or the code for the exploit?
A. No.
Q. Have you looked at the server component?
A. I have not looked at the server component, but as I stated earlier, I did look at the code that generated the identifier. I don't know if you want to call that part of the server or not.
Q. I understand that things can sometimes overlap, and it's not always easy to make different hard and fast boundaries between various components; is that fair?
A. That's fair. In fact, I might include in that overlap the packet traces because that includes responses from the server.
Q. Now, in your declaration, in paragraph 3, you forthrightly disclose that you did not review the source code or executable for the exploit that deployed the NIT payloads. I have that on the screen. Is that, in fact, from your declaration?
A. That appears to be from the declaration.
Q. You referenced -- you used the word "payloads" plural?
A. Well, there are three cases involved here, and there were

three payloads that were given to me.
Q. On page 4, line 1, of your declaration you reference payloads that were generated in connection with this case. Do you recall that?
A. I don't. Do you want to point me to that line in my declaration?
MR. FIEMAN: Your Honor, I am referencing docket 58-1. All my references are to Tippens dockets for clarity, Your Honor, and this will be on page 3, paragraph 4, the last line, carrying over to page 5. If I may approach the witness.
BY MR. FIEMAN:
Q. Do you have a copy of your declaration with you?
A. I do have a copy in front of me.
Q. I just want to read that sentence into the record -- and correct me if I am misreading it -- "The bespoke payload" -- that means sort of the custom payload for this operation, correct?
A. Yes.
Q. Okay -- "carried a unique identifier that was generated by the FBI" -- we've already talked a little bit about that -- "as well as a case identifier common to all payloads generated for the Playpen operation." So again, there's a reference to two things there. One, multiple payloads and secondly, them being generated for the individual cases.
Now, my question is, were there multiple payloads that

were used in connection with this NIT?
A. So to clarify what I meant in my statement is that I was given the three payloads. I am referring to those Playpen payloads that I was given. They were different because each one, as I indicated in the declaration, contained or had embedded in it these unique identifiers. So that's why I used the word "generated." It's the embedding of the unique identifier.
Q. Thank you. Professor Levine, do you know who wrote the code for the payloads?
A. I don't.
Q. Do you know when it was written?
A. I don't.
Q. Do you know if it is the same or different from the NIT payloads that were used previously in Operation Torpedo?
A. No, I don't.
Q. Now, just to back up for a second, on your slide that dealt with NIT investigative techniques, you had indicated while mapping the route of the NIT that the NIT was downloaded by the user at some point in this investigative process; is that correct?
A. I see that on the slide.
Q. And that would have been done, based on the information you have about this case, without the user's knowledge; correct? It was done in secret?

A. Based on the information I have in this case, that's correct.
Q. I don't really want to debate whether this is malware or not in our terminology, but it is fair to say that commonly, when we talk about malware, it is fair to describe it as code through some method of access to a computer, without the user's knowledge or consent, performs functions on the affected computer that the users did not know or want?
A. Are we talking about the NIT or are we talking --
Q. We are talking about malware in general.
A. Okay, so we are changing from the NIT?
Q. Yes, that's why I was saying in general at the beginning of the question.
A. Sure, those are among the components of malware.
Q. Thank you. Now I want to spend some time focussing a little bit on the exploit component, so that's where I am going next.
As I indicated, I understand that you want to distinguish between the various components as much as possible to keep things clear; is that correct?
A. The components of the NIT, yes.
Q. Is it fair to say that it's called "Network Investigative Technique" because these components work in conjunction with each other?
A. I didn't invent the terminology. When I referenced

Network Investigative Techniques, I am talking about this entire process, so that it's clear to the Court.
Q. Well, based on your knowledge of this process, is that fair, that these components work in conjunction with each other and all together they make up the NIT?
A. Yes.
Q. Now, do you agree or disagree that the exploit, the exploit component, can make fundamental changes to a computer's data and disable its security settings?
A. So, again, I haven't examined the exploit, so just speaking generally, when I say the exploit, I am referring to the method of entry that allowed this payload to execute. As I said in my earlier testimony, I can speculate that this exploit may leave some changes behind or it might not.
Q. So again, this is actually a statement from earlier testimony by Agent Alfin that an exploit can make -- and we are speaking generally -- can make fundamental changes to a computer's data and disable its security settings.
Do you agree or disagree with that statement?
A. If I interpret the statement to mean can or cannot, then yes, I agree.
Q. It can do those things. And you have not seen the exploit?
A. I have not seen the exploit.
BY MR. FIEMAN: And just for the record, Your Honor,

this is in our exhibits, but I am referring to testimony that's before the Court on the screen from Agent Alfin on October 11, 2016.
BY MR. FIEMAN:
Q. So you are in agreement with Agent Alfin that it's possible for exploits to do those things, make fundamental changes to data and disable security settings?
A. The exploit is undefined as a piece of software, yes, it's possible or it might not.
Q. Correct. We don't know. You don't know because you have not seen it, correct?
A. I have not seen it.
Q. Neither have we, so there we are. In fact, I think Professor Miller -- you've reviewed his declaration that was submitted originally in the Michaud case but also in connection with this case?
A. I believe we are referring to the same declaration. I read the one I referred to in my declaration.
Q. Just for the record, there's only been one declaration.
A. That's the one I read.
Q. I promise you I will try not to lead you down the garden path on records you have not seen.
So in Professor Miller's declaration -- I have it on the screen now, paragraph 4 -- he makes a couple of statements, and again, I am trying to find areas where we can agree.

A. Uh-huh.
Q. He says that "a computer system that has been exploited has been fundamentally altered in some way," and he goes on to talk about how, as a result of that, "the computer may crash, lose or alter data, not respond to normal input or it may alter any of the settings on the system. Depending on the exploit, it can affect the security posture of the computer going forward."

Now, do you agree or disagree with that summation?

A. I don't agree with the entire quote that you've provided.
Q. And I understand that your disagreement may arise from the fact that you've described to the Court the exploit as a key, correct?
A. Can I tell you how I disagree?
Q. Absolutely.
A. So this first statement is very absolute. A computer system that has been exploited has been fundamentally altered in some way; it may or may not have. We don't know. So I will give you an example of an exploit that does not fundamentally alter a computer in some way.

I may approach you and I may call you and say, oh, I'm here -- I am sorry, I don't want to use you as an example. I may approach someone and say: I'm here with your child. I really need to know the password to your email because your child needs to go home. I get the password and I log in as

normal. There's no alteration to the computer. That's a method of access that does even not touch the computer. So I think that first statement, first of all, is way too broad.
Q. It's broad, in fact, because at least the defense experts don't know what this exploit looks like, correct?
A. No, I don't agree that that's a description of my reasoning.
Q. Okay. You are aware that we have not seen the exploit, correct?
A. Yes, I am aware of that.
Q. You have not seen the exploit?
A. I have not seen the exploit.
Q. So by some standards, some generalization is inevitable given that we don't know what this actually did, correct?
A. Yes.
Q. As a generalization, do you agree with Professor Miller's statement that exploits are capable of doing all of these things?
A. I agree with the statement that they may alter -- may alter -- any of the settings on the system. If that's what you are asking me, I agree with that.
Q. And also delete or lose or change data, that may happen as well?
A. If that's part of the method of entry. I am restricting the exploit to the method of entry. If you are referring to

what happens after the entry, yes, it's also possible after the method of entry to then crash, lose or alter data.
Q. Well, both Agent Alfin in his October 11th testimony, and Professor Miller, are speaking specifically and directly to exploits. Now, I understand you may not agree with them, but you aware of the context of their statements, correct?
A. Yes. I don't think we disagree. I think you are right, I think we maybe have a disagreement about definitions. But I agree that these things are all possible on a computer for software that can run.
Q. That possibility is -- certainly in a case where an exploit does that, it's much more than a key, correct? It's actually not just going into the house, but moving the furniture or shredding documents, altering data or leaving the door open for other people; that's more than just a key if the exploit is doing that?
A. So the way you've described it is beyond the method of entry. If you move around the furniture, then yes. As I stated, malware can have multiple goals, or rather have multiple components. One of them is the method of entry, and the other would be what it does once it gains entry. So that would be, for example, altering the data perhaps maliciously. So if you would like to put this all together in the components of malware, I certainly agree with that.
Q. Well, again these statements from both Professor Miller

about the exploit component -- I understand that you don't necessarily agree with them in their entirety; is that fair to say?
A. I agree with them in parts, and I think -- I agree with them because if I realign what they are saying with my definitions -- for instance, as I stated, in order to gain entry, some things may be done, there may be malicious activity afterwards. These components can happen on the system. I agree.
Q. And I you understand why you want to use your definitions, but you can understand why we are concerned about maybe the definitions that Agent Alfin and Professor Miller are using and where these boundaries might be drawn, correct?
A. Yes.
Q. Now, in terms of the exploit being restricted and just being a key in this case, you are basically relying on information that's provided to you by Agent Alfin, correct?
A. Yes. There are various statements from the declarations that I rely on to do this.
Q. In fact, in paragraph 9 of your declaration, this is one example where you say we know from Special Agent Alfin's sworn statement that the exploit was restricted to allowing the payload to be delivered and executed, correct?
A. Yes, I wrote that.
Q. So is it fair to say that the entirety of your information

about what this exploit did or did not do, comes from Agent Alfin's declarations?
A. Yes. I mean, "entirety" is a strong word there. If you want to talk about the quote that's up here --
Q. I just want to know about your personal knowledge, if any, about what this particular exploit did or did not do. That's all I am asking about.
A. You are correct.
Q. All right. Now, setting aside what the exploit did or did not do and what we may or may not know about it, let's talk a little bit about what we might be able to find out about what it did without looking at the exploit itself?
A. Uh-huh.
Q. I think you testified earlier about how you would expect that if there were changes, if there was some kind of change to the security settings or lost data, you should be able to kind of reverse engineer it from the client's hard drive?
A. That's not what I said.
Q. Okay, then please correct it.
A. What I said was that in the case of a method of access -- what I was referring to was malware. So in the case of the method of access from malware, it may have left a trace. It may have altered things. It may not have left a trace, okay. So in the first case, if it doesn't alter anything, an example of that is the phone call I gave before, then there's nothing

to do there.

In the other case, the malware or method of entry might alter the computer. So if on another computer you see those same artifacts, you might conclude that that same method of access was used. And then I also clarified that that does not tell you any of the following activities since different software could reuse that same method of access.

Q. All right. So let's just use the word "malware" broadly. You had indicated in paragraph 16 of your declaration that, assuming for the sake of argument that the exploit did something to the computer beyond just opening it, you would expect -- and I am looking at the last sentence -- that "such malware would need to reside in permanent storage, making it easier to find by experts, and yet it has not been found."

Is that an accurate statement of your declaration?

A. Well, the full quote is --

Q. Please read it.

A. Okay. "It is reasonable to expect that malware designed to furtively store images on the defendants' machines would also have the ability to later retrieve the images."

So here, I am talking about a specific kind of task for that malware. The task I am referring to is both the storage and retrieval of the images. So within the context of that task, what I write next is, "In order to allow retrieval after a device reboot, in that case storage retrieval after a device

reboot, the malware would need to reside in persistent storage, making it easier to find by experts."

So what I am saying is, this particular type of malware, for instance, it might store child pornography, has not been found, to my knowledge.

Q. We are going to talk a little bit more about that, and particularly about the reboot. But I do want to stick with these general principles about computer code or malicious code that may be on a computer before we get to specifics.

A. Okay.

Q. Now, Agent Alfin has also testified -- this is again attached to our pleadings. He was asked earlier about malware in general --

A. Uh-huh.

Q. -- and was questioned about whether programs can be written so that there is no code left behind on the computer once that information has been sent somewhere else. Do you understand the question he's being asked?

A. Yes.

Q. He answers -- this is on a separate slide. Agent Alfin there is agreeing that malware can be designed so in fact there is no code left behind on the computer that can show that it was there, tell a forensic specialist like Robert Young what it did or all those other things that may be important to know.

A. Are you asking me a question?
Q. If you agree or disagree with that statement.
A. I don't agree with what you said. I don't think that's a fair reading of the quote in front of me because I believe you skipped an important phrase between the two hyphens, the end dashes.
Q. He is talking here about the information designed to steal someone's information, correct?
A. He's talking about malware is generally designed if you are going to steal someone's information -- and I would like to point out that is a different scenario than the quote you took from my declaration, which was about malware that's stored and retrieved after reboot -- that information, stealing someone's information and then leaving doesn't require you to stay there.

So that's why such malware could delete itself. But if I am going to write malware that stores images on someone's computer, and I would like to later retrieve it, then I do need to stick around because how can I respond to commands that request retrieval?
Q. Well, you are aware, are you not, that the malware in these cases, the NIT components -- excuse me, because we don't need to agree on the word. The NIT components were deployed against the various defendants in these cases back in February and early March of last year; are you aware of that timeframe?

A. That's what I understand.
Q. Okay. And just in terms of malware in general, whether it's to steal somebody's information, alter or delete files, create a remote storage for pornography, do you agree or disagree that any of those types of malware may be written so that there's no code left behind? Is that possible?
A. No. Again, you are including in that the type of malware that would store and then retrieve. So in order for the retrieval to work correctly, I don't see how the malware could --
Q. I am not talking about retrieval --
A. I'm sorry, could you clarify your question?
Q. I'm talking any type of malware that either alters or changes data, alters or changes security settings, stores unwanted data or images on a computer remotely, any of that type of malware, whatever its malicious purpose may be, is it possible for code to be written, the code itself, that does not leave a trace on the computer?
A. For the examples you just gave, yes, it's possible.
Q. For all those examples, correct?
A. I believe so, as I understand you to say them.
Q. Now, in this case, you actually indicated that at least some of the NIT code -- and again, these definitions are hard, but whether it's the exploit or the payload, some part of the NIT code may not have been left behind on the target

computers; is that a fair statement?
A. Well, I haven't examined those computers, but given that you are requesting this information and you have those computers, I assume that you don't have access to that information.
Q. Well, in fact you wrote -- if you will turn to paragraph 4 -- excuse me, paragraph 4 on page 5 of your declaration --
A. Uh-huh.
Q. Turn to page 4, lines 7 and 8. It's the last sentence, "The exploit and payload did not persist on the defendants' computers after execution."
A. What's your question?
THE COURT: Just a minute, counsel, where are you looking?
MR. FIEMAN: If you look at docket 58-1, Professor Levine's declaration on page 4, Your Honor, it's lines 7 and 8.
BY MR. FIEMAN:
Q. Now, in reference to the NIT in this case, you state that, "The exploit and payload did not persist on the defendants' computers after execution"; is that correct?
A. I state that because I am assuming that if they were there and available -- what I mean by "persist" is there and available -- you would not be requesting them from the government.

Q. Okay.
A. So by persist, I mean they are not available or ready made for you.
Q. Did you look at any of the defendants' hard drives or data storage devices in connection with this case?
A. I did not.
Q. Did you ask to get a mirror image hard copy or do that at any point?
A. I did not. So you are right, that's a logical conclusion.
Q. I am not impugning your logic. I just want to follow it. Again, you indicated that you had read Robert Young's declaration in connection with this case?
A. Yes, I read that declaration.
Q. And in paragraph 7 of his declaration, he talks about some of the things that may have gone on, given the NIT on the defendants' computers, and that may include instructions that mask or conceal the object code -- we'll talk a little bit more about that -- but basically the code, making it possible to reverse engineer the code, and he also talks about encryption and some technical things that are already kind of over my head. And then he also talks about that some data may even be lost when a program ends or is shut down or rebooted.
Again, these are generalizations, but do you dispute any of his description of some of the challenges that would come with trying to work backwards from the defendants' devices?

A. So, putting aside disagreements about what the NIT is, so let's talk more, as you said, as you suggest, let's talk about the exploit and the payload. If the exploit is not available to you, than yes -- sorry, did I say that correctly? The payload is available, and so looking at that material is not as hard. But yes, the exploit, which is not available, would have -- I am not sure of your question. You are asking if that exploit is still available on the defendants' computers, could it be reverse engineered, would there be challenges in discovering it, yes. Possibly, yes, presumably because you haven't found it.

Q. If you are having trouble keeping track of terminology, imagine the trouble we are having, but I appreciate your efforts to clarify.

Now, you did spend a fair amount of your declaration talking about sort of in general well, we don't need the NIT -- all the NIT components, there's some we have got and some we haven't. We don't need all of those because again, you would expect to be able to find evidence of what we are looking for on the storage devices of our clients. Is that a fair general statement of what you talked about at some length?

A. Yes, because if what you are looking for is third-party malware that's responsible for evidence that's found on the computer, that's not related to the method of entry.

Q. It's not what we are looking for. That may be part of --
A. Could you clarify that?
Q. We are looking for what the NIT did. That's what we are trying to figure out.
A. You are looking for the method of access?
Q. We are looking for whether the exploit, as you previously agreed, could have changed or altered data or changed security settings, for example.
A. So you are looking for the trace that might be left behind from an exploit that ran and had a method of entry?
Q. We are looking for the exploit to know what it is.
A. You are looking for the task that occurred in the payload?
Q. We are looking for what the exploit is.
A. So you are looking for the method of entry?
Q. No, we are not agreeing about that because --
A. I agree.
Q. -- I think we already agreed, based on the prior statements, that some exploits can change data, correct?
A. Some methods of entry might change data, yes.
Q. Now, just in terms of -- just finishing up with this problem of trying to work backwards from our clients' devices, I want to direct you again to some testimony from Agent Alfin that has been provided to the Court as part of the *Jean* transcript on October 11, 2016.
Again, we are talking in general just about some of the

data analysis problems that attend this type of case, whether it's an NIT case or malware case, however you want to define it, okay. And there was a question that was directed to Agent Alfin about: "Are you familiar with what happens to data on a computer over time that's become overwritten," correct?

And the answer there is: Yes, among other things, when the computer reboots, it's going to clean up data files, which I understand may change or delete or compress files, correct?

A. Depending on the operating system.

Q. Depending on the operating system. So again, continuing with Agent Alfin's statement, so if there were changes to the computer -- and I think we are referencing a defendant's computer -- "eventually they can be corrected or deleted or removed." Does that seem like a fair general statement to you?

A. Yes, it could be.

Q. Also, if you update your operating system, there may be changes to the data?

A. Which data, the user data or the operating system data?

Q. Data that is stored on the system.

A. Certainly, the operating system data would be changed if that's what was upgraded.

Q. So computers are inherently rewritable and changeable all the time; is that a fair general statement from Agent Alfin?

A. General purpose computers do general things, absolutely.

Q. Now, there's a reference, as the testimony continues, to the *Cottom* case. Have you heard that case referenced?
A. Only in the declarations that I have read.
Q. Just for clarification, that was one of the cases that involved Operation Torpedo -- I don't expect you necessarily to know that, but clearly, you can see from this question and answer that Agent Alfin is referring to a prior case involving an NIT, and he was asked: "You testified that in the *Cottom* case, the software that you analyzed didn't make any fundamental changes?"
Do you see that question?
A. This is a question to Agent Alfin?
Q. Yes.
A. Okay.
Q. And I am going to ask at the end if you agree or disagree with that statement.
MR. BECKER: Objection, just briefly, Your Honor. I think this may just be an error. I don't believe this is Agent Alfin's testimony, and I would just ask if counsel can clarify. I think this is Mr. Miller's testimony.
MR. FIEMAN: I will double-check the record, but it doesn't matter if it's Agent Alfin or Professor Miller -- and I will clarify it at the break --
MR. BECKER: I think it doesn't matter in terms of the clarity of the record, but I do not believe this is

Special Agent Alfin's testimony.

MR. FIEMAN: I will double-check the excerpts.

THE COURT: What's the question to the witness?

BY MR. FIEMAN:

Q. Do you believe that it's possible to know whether there were fundamental changes to the computer as a result of an NIT without it having been analyzed?

A. I don't have access to the *Cottom* case. I don't have the materials. I am not sure what you are asking me. If you want, I can read this and then try to agree with it, but I am so uninvolved in the other case, I am not sure what you are asking me.

Q. I am going to move on because I think we also need a clarification. But let me focus on an issue just in terms of the payload components at this point. We talked about exploits and malware in general. Now I want to talk about the payloads.

A. Okay.

Q. I am going to need some help because I have never taken a computer class, and I don't know code. But I understand certain general principles as this: Broadly speaking, there are two types of code, source code or code that is initially written by a programmer, correct?

A. You said there were two types?

Q. Well, is that one type of code, source code?

A. The original source code, yes.
Q. And is that also sometimes known as human-readable code?
A. Yes, that's an example of human-readable code.
Q. And then there is a different type of code that's called sometimes object code or binary code, correct?
A. Yes, the result of compilation.
Q. When you say compilation, if I understand the process, you'll have a programmer write out the code in a programming language. That human-readable written code will then be converted into zeros and ones, binary language which will give the computer instructions to run. Is that a fair generalization?
A. Yes, absolutely.
Q. So if you know -- if you have the source code, and you know the programming language that was used to write it, you can go through and analyze it and understand what the code instructed the computer to do or not do, correct?
A. You can certainly try.
Q. But with binary code, that's often referred to as not human-readable, correct?
A. Well, there are fewer experts who can take care of it, but yes, it's definitely not as easy as human-readable code, the binary code. You can run it, which is a nice advantage over source code.
Q. Now, you said you reviewed human-readable code in

connection with the payload; is that correct?
A. On the stand here today?
Q. Yes.
A. So what I was referring to is, embedded within the payload there is scripting language.
Q. What is scripted language?
A. There was particular human-readable code, I believe it was called the bash script. I don't know how technical you want me to get, but there was a script embedded inside the executable, at least one of them.
Q. What about non human-readable?
A. There was also non human-readable code in there.
Q. So if I understand your testimony correctly, you testified that you looked at and analyzed the payloads, correct?
A. I did.
Q. And you looked at human-readable code, right?
A. There was some human-readable code embedded in it.
Q. There was also, however, other code that was not human-readable?
A. There was human-readable code, there were pieces of text in the code, and there was compiled code, this object code that you referred to. All three were in there.
Q. What did you do with those portions of the payload code that were not human-readable?
A. I didn't read them.

Q. You didn't read them?
A. No. So let me clarify. So I didn't -- they are not as easy to read as you would say. I looked through them. I extracted the text that was embedded in that quote-unquote non human-readable code, and that text corresponded, for example, to the unique identifier that I saw -- or other output that appeared in the packet traces.
Q. So you were able to read part of it?
A. I was able to read part of it; only part, as you are saying.
Q. Previously, you had testified that you analyzed the payload code, but only those parts you could understand; is that correct?
A. Yes, I apologize. To clarify, as part of my analysis, I extracted the human-readable code. I apologize if that was not clear.
Q. So there are, consistent with Mr. Tsyrklevich's declaration, parts of this payload that, at least according to your testimony just now, are not in a human-readable format?
A. They are not in a human-readable form, but they can be executed. For example, there are people who can read this, let's say, a computer scientist readable code. It's not impossible to read the code. I didn't do it. I didn't do it. But it's not impossible to do. And you can run it. It's not a dead-end, but it's certainly challenging, I agree with you.

Q. It was a dead-end to you, though --
A. It was not a dead-end. I didn't elect to do it. I didn't find it necessary because my concern was whether or not the exploit would help me, and I didn't see how reviewing the payload more than I did was necessary at the time.
Q. That was your opinion of what was necessary or not necessary?
A. When referring to the exploit, I found that, as I testified earlier, for example, reviewing the exploit would not tell me whether the packet traces would return correctly, it would not tell me whether the identifier was created without error. It would not tell me whether malware was run on the machine using the same method of entry. It would not tell me whether the payload was delivered without error as it was with Tor. So those questions didn't seem relevant to going further than I did at the time of the payload. But that doesn't mean I couldn't have gone further.
Q. But you understand, it's ultimately for the judge to determine what may be relevant or not relevant for the --
A. Just the questions I personally was trying to answer, I wouldn't presume.
Q. They were fairly limited, right, because you didn't ask to see the exploit, correct?
A. I didn't ask to see the exploit.
Q. Okay. And you didn't deal with the non human-readable

parts of the payload, correct?
A. I did deal with it. For example, I extracted text from the non human-readable parts that I could see corresponded to the packet traces.
Q. The extract part, but there are lots of parts --
A. There was lots of other parts that I did not.
Q. What about the server component? Did you look at the server component?
A. I did not. We discussed the authority. The only part I saw was the source code that generated the identifier. I don't know if we are calling that part of the server or not. I did not look at the parts that weren't related to -- now, however, I did see the output of the server because that's contained in the packet traces --
Q. Okay.
A. -- and that's available for anyone to inspect.
Q. We'll get to that briefly. Robert Young, in his declaration at paragraph 5, talked about this problem between human-readable code and non human-readable code, and I take it you don't really have a disagreement with his assessment of the problems in trying to deal with non human-readable code at the back end of the defendants' --
A. Do you mind if I read the statement?
Q. No. I am sorry, I thought you already reviewed the declaration.

A. I have reviewed it, but I would like to see it again.
Q. Take your time.
A. Yes. This is absolutely factually true. The computers function on an object code. Everything he says here is true. Object code is created by taking human-readable source code. This is the standard process by which programs are created. So did you have a question other than --
Q. No, I just wanted to know if you had any disagreement with his assessment --
A. Of how computer programs are generated --
Q. And then he goes on to talk about --
THE COURT: Just a minute. You are talking over each other. Let's go by question and answer. Go a little slower.
MR. FIEMAN: Thank you, Your Honor.
A. Can we start again? Can you reask the question?
BY MR. FIEMAN:
Q. Just to wrap this up, you also understand that I use the word "reverse engineering" or trying to figure out what the source code is from the binary code is a difficult or at times impossible process?
A. Generating the source code from a compiled program can be difficult in some cases, not in others. For instance, Java, the compiled code, pretty much looks exactly like the source code. The script that I extracted from the binaries, which is only part, was exactly human-readable. But yes, absolutely,

it can be the case that compiled code can be obfuscated in such a way that you can't reveal the source; however, that is not what the statement in front of me is referring to.
Q. Let me ask you this. Let's say you've got a manual for a foreign car, a BMW, and part of it is in English and the rest is in German --
A. Uh-huh.
Q. -- and you can only read English?
A. That's true.
Q. Do you think you have a complete idea of how your car operates or how to repair anything that may go wrong with it if you can only read the English parts?
A. Well, I still have the car, so I can drive the car and use my experience to see -- my general experience to see how cars operate and go with that.
Q. Correct. But --
A. But yes, your question is would the manual tell me everything? Certainly. I couldn't read the German parts. That's true, I don't read German.
Q. Now, I just want to talk a little bit -- and we are getting close to the end -- about the delivery and routing of the information on the internet in general and then more narrowly within the Tor network --
A. Okay.
Q. -- and follow-up a little bit on the slides you presented

earlier.

This is from paragraph 8 of your declaration. You made a conclusion in paragraph 8 about the delivery and integrity of the code, and you stated that "it stands without doubt that the exploit and payload were delivered with integrity because connections to Playpen were accepted only by a tamperproof connection created and maintained by Tor," and you are correct, nobody disputes that part. Is that an accurate summary of your statement?

A. That is my statement.

Q. Okay. Now, you are aware, however, that not all of the data involved in this case traveled or resided solely on the Tor network, correct?

A. For example, the results of the payload were returned outside of Tor?

Q. Yes. They were returned on the open internet, correct?

A. That's correct.

Q. Now, this has also been provided to the Court. I just want to talk generally about the benefits of using encryption or like the Tor network, an encrypted network, for transmitting information.

Would you agree that there are benefits for sending information through the internet on an encrypted connection?

A. Yes.

Q. Does that prevent tampering?

A. It's one of the ways to prevent tampering; it's not the only one.
Q. But it is one fundamental way to use encryption, correct?
A. Correct. It's not the only one.
Q. You are aware that the data that was collected from the defendant's computer was not encrypted when it was sent from the target computer to the FBI server, correct?
A. My examination of the packet traces show that, you are right, that the payload return packets through this TCP connection, but it did not use encryption.
Q. Is it fair to say that even such basic services or companies like banks and credit card companies and things like that generally use encryption as a security method?
A. Yes. Actually, could I restate the previous question? Would you mind going back?
Q. Maybe we should have it reread because I will probably --
A. Forget?
Q. -- forget what I was going to ask previously.
A. You asked me if we could use encryption.
Q. I am asking if the part of this delivery and return that went from the target computers back to the government server where the data was collected, the IP address, was that portion of the transmission over the open internet?
A. I'm sorry. Yes. I don't want to change anything. That's correct. My apologies. It was on the open internet.

Q. Now, then you talk about these packet capture traces -- and I think it has got a little bit something -- and please correct me if I am wrong, but I think it has something to do with the data stream or the transmissions on the open internet?
A. Yes, that's exactly what that is.
Q. You analogized your assessment of the security of that part of the process based upon kind of "to" and "from" addresses for the data, correct?
A. Yes, uh-huh.
Q. And I just want to give you a very simple analogy and see if I understand this. So it's a little bit like if I place an order with Amazon for delivery of a pair of sneakers --
A. Yep.
Q. -- and they are put in a package by Amazon and the package is delivered to my door, and we know the package got there because it's being sent from Amazon, and we have a delivery receipt to me, correct?
A. Yes.
Q. Does that basically coincide with what you were describing in your declaration?
A. Using your analogy, can I add one more detail?
Q. Go ahead.
A. So you said I ordered something from Amazon. Sometime later, it's delivered to my house. And then Amazon knows that

it's been delivered and so on. But part of that delivery would be a tracking number. Now, let's say I haven't received my materials yet. Amazon may say, why don't you track your package? So what do I do? I go to the -- let's say Fed Ex was delivering it. I go to the Fed Ex website and they say which package would you like to track?

Now, I can input everything in there, but I have to get a very long tracking number to get the package that's going to my house. There's no encryption perhaps on that connection but could my neighbor guess my package? Not a chance.

Q. But really, my question is a little bit different.

A. Okay, but I think that's what --

Q. That's a fair statement. I think that's fair. You got the to and from information. But, Professor Levine, do you know what's in your Amazon package until you open it? Do you know if they sent you the sneakers or sneakers at all?

A. No, I don't.

Q. That brings me actually to the server component here, and I just want to make sure -- confirm that you have not looked -- setting aside the identifiers which you agree are at least related but separate -- you have not looked at the server component, correct?

A. I have looked at the output of the server component, which is in the packet traces.

Q. Right. Which is that address information, correct?

A. Which is the complete packet trace including the address information and the responses by TCP and so on.
Q. Now, this is just my final question.
BY MR. FIEMAN: It's from, Your Honor, docket 31-2, Mr. Tsyrklevich's declaration.
BY MR. FIEMAN:
Q. I am just going to ask you about Vlad Tsyrklevich's statement regarding the importance of the server component, and this will be my last area --
A. Okay.
Q. Mr. Tsyrklevich states on page 3 of his declaration that "it is the server component that stores the identifying information returned by the payload, and it must faithfully store and reproduce the data that was sent."
Do you agree or disagree?
A. I agree, but may I ask you, if you have a slide with that statement, would you put it up?
MR. FIEMAN: Can we switch to the screen, Dara? That will make it much easier for everybody.
A. If you wouldn't mind, could you repeat the question?
BY MR. FIEMAN:
Q. It's actually the bottom paragraph we are focussing on. The server component is what stores the identifying information returned by the payload and "must faithfully store and reproduce the data it was sent." Do you agree or

disagree, in generalization?
A. Yes.
Q. Then he goes on to talk about some of the things related to the server component that he was concerned about, including the correct use of data storage -- I frankly don't even know what that is.
A. Well, for example, the checksum would be something that would ensure that the data storage primitives were done correctly.
Q. That's an example?
A. That's an example.
Q. And the programming practices used on the component to avoid corruption, tampering and things like that. And then he talked about this in terms of the digital chain of custody; is that sort of a fair analogy?
A. Is digital chain of custody an important concept in this case? Absolutely.
Q. He concludes -- at least Mr. Tsyrklevich concludes -- that without the missing data, basically the server component, "I am unable to make a determination about the various chain of custody issues."
A. Well, I believe he -- are you asking me a question?
Q. I am asking if you've read that and if you disagree or agree with Mr. Tsyrklevich's assessment?
A. I agree that chain of custody is an important part of

these cases. I believe that this chain of custody is available for review in the information that was provided, in particular the information returned to the server is exactly what is in the packet traces.

Additionally, as a redundancy, there's also the report from the FBI about what was received. Those values match, and I have no reason to believe anything about the integrity of what's in the packet traces. So in fact, the chain of custody is available for review, and I have done that and I believe it was maintained.

Q. But Mr. Tsyrklevich at least believes that the server component is an important part of this chain of custody?

A. And he does say that. Unfortunately, we have both the packet traces to see what the server received. Effectively, we don't even need the server. We know what was received, and we also have a report from the FBI of what they received. They happen to match. There's no reason to doubt, therefore, that any chain of custody was broken, nor that the data was tampered with along the way because the checksums would show that kind of alteration by a router --

Q. Okay. So I fully understand this, you are satisfied with the information that's been made available to you in terms of the chain of custody --

A. And I believe it meets his needs.

Q. Well, Mr. Tsyrklevich at least is addressing here the fact

that the server component is an essential part of the chain of custody process, correct?
A. He's stating that, and I believe that's a failure on his part to not take advantage of the packet traces that were made available. Perhaps if he had evaluated them, he would have been able to conclude differently and this statement would have been satisfied about his chain of custody.
Q. But they were available to Mr. Tsyrklevich and he deemed that would be insufficient without access to the server component?
A. How would he know without looking at them?
Q. Because it's like saying you get half a puzzle in a box, you are not going to know the picture unless you get the other half. Is that a fair way to put it?
A. No. And I can give you a counter example, if you'd like. So for example, we don't know -- for a time, until the source code was released for the identifiers, for generating the identifiers, we didn't know exactly how they were identified.
But I gave the example of, without that code after the fact, you could look for duplicates and validate that no matter what algorithm was used, that process was completed reliably. So I believe here is another example where, even though we don't have the server code, we do have the exact information that was sent to the server. There is also no mysterious algorithm being performed at the server that is

under dispute. There's no secret at the server --
Q. How do you know that if you haven't looked at it?
A. Because you don't need to know what happened at the server other than the fact that the information was sent to it from the packet traces. We know what the server received. We know what the server generated. We have the code for it. I don't see -- can you clarify for me what he would get out of looking at the server code?
Q. I am not the expert here. I am just going by Mr. Tsyrklevich's --
A. I am sorry for interrupting.
Q. He deals with the identifiers in the first bullet point, correct?
A. He does deal with it in his paragraph. In my declaration, I dispute what he says.
Q. You dispute Mr. Tsyrklevich's assessment of the importance of the server?
A. No, that's not what I just said. If you could put the slide back on. You asked me about the paragraph where he talks about the --
Q. Which paragraph?
A. I believe you are talking about the bullet on what looks like 15.
Q. The first bullet or the last bullet?
A. I believe you asked me about the first bullet, which is

13. So I agree that he talks about unique identifiers in that paragraph. What I don't agree with is that this is a cryptographic operation. That's what I was starting to say. It's factually not a cryptographic operation.
Q. Again, you are sort of getting a little bit over my head. Let me just ask one final question. Mr. Tsyrklevich clearly states -- and I understand you may not agree with him --
A. I might.
Q. -- that he needs to see the server component, and you say he doesn't. Is that a fair summary?
A. I believe that the chain of custody can be validated based on the information that the server received. He may also like to look at the server code, but it is a redundancy. It's not a necessity.
Q. Well, he didn't say he'd like to do it, he says he's unable to make a determination without it about the integrity of the data. Do you disagree with that statement?
A. I believe he's correct, because he did not look at the packet traces. So his statement is correct in terms of what he did and didn't do.
Q. All right.
MR. FIEMAN: No further questions. Thank you, Your Honor.
THE COURT: Mr. Becker.
REDIRECT EXAMINATION

BY MR. BECKER:
Q. Professor Levine, starting with the last topic of questioning from cross-examination. In the Tsyrklevich declaration, did he point to any fact or evidence that suggested that there was a problem with the digital chain of custody that you've talked about?
A. No, not to my knowledge, not to my recollection.
Q. In terms of the security, you were asked some questions about the TCP connection, its security and encryption. In terms of evaluating how secure that connection was, does that evaluation have anything to do whatsoever with review of the exploit and method of access?
A. It has nothing to do with it, because it's a process that's related to the payload and the execution of the payload.
Q. You were asked some questions about computer code being human-readable or not human-readable. Is code that is not human-readable, testable?
A. Absolutely, it's testable. It's runable on a computer, and you can even -- as an expert, you can even follow the code and read it. I myself, like many people who have computer science degrees -- the second year of my undergraduate program, I took a course on programming in "human-unreadable" code. So I have written an entire program, as probably any computer science major with this type of code. In fact, the

compilers that generate this other code were written by humans. There are people who do this. It's testable. It's readable. It's just not as easy as reading a book.
Q. And so in the form that you reviewed the payload data, is that in a form that could be tested in the sort of manner as you suggested?
A. It could be run again and again on a variety of computers, as many times as they would like or any tester would like. It can be compared to the output of the packet -- it can be compared to the packet traces specifically, is what I am referring to and compared to contrast it.
Q. Would you need to have the method by which that payload information was delivered in order to conduct that sort of testing?
A. No, you don't. As I said earlier, when someone breaks into your house, that doesn't answer what they did when you know what they did, it doesn't tell you how they gained entry.
Q. Thank you.
MR. BECKER: No further questions, Your Honor.
MR. FIEMAN: Nothing further, Your Honor. Thank you.
THE COURT: Just a minute. I have a question, and I guess this is to counsel. Mr. Levine or Dr. Levine --
THE WITNESS: As you prefer.
THE COURT: -- he indicated that the exploit and the payload were two different things. I've lost track of what

you all have because you've got some new information here.

Do you have information on the payload, as opposed to the exploit, or are we just talking about the exploit?

MR. FIEMAN: No. We are talking about three things at this point, Your Honor. The exploit, which we disagree about its functionality. We have gotten readable parts of the payload. As you refer back to Mr. Tsyrklevich's declaration, he received some information that actually started this whole thing.

THE COURT: You are telling me you don't have full information that you want on the payload?

MR. FIEMAN: Well, the problem is -- and we also disagree about what's readable or not readable, and we are actually just learning -- over the past week, I asked Mr. Hampton about this just this past week -- that there are not human -- there are human-unreadable portions of it, and we are trying to clarify what that means and who's seen what. I honestly don't know at this point, except based on Mr. Tsyrklevich's record he received some readable portions.

THE COURT: Okay.

MR. FIEMAN: So we are missing the exploit. We will go back and revisit -- I can sort out our terminology about the payload, but regardless we are still, no matter what, absolutely missing the exploit and the server components. And that has not changed since Michaud, Your Honor.

I hope that answers your question.

THE COURT: Okay. Thank you. You may be excused.

THE WITNESS: Thank you, Your Honor.

THE COURT: Any further evidence to offer on the first motion?

MR. BECKER: Not from the government, Your Honor.

MR. FIEMAN: No, thank you, Your Honor.

THE COURT: All right.

MR. FIEMAN: Your Honor, I would beg one caveat. We had represented in our pleadings that Mr. Young did in fact go back and try to do this reverse engineering on Mr. Tippens's hard drive. We had represented in our pleadings that Mr. Young had received a copy of Mr. Tippens's laptop hard drive and did make the attempt to reverse engineer, as we are calling it, and was unable to do that. He is in court and can confirm that if you need confirmation, but that statement in my pleadings is saying that.

THE COURT: I am mindful of the hour. I assume the next step is some argument on this motion, and I assume that the sensible thing is to start that at 1:30.

MR. FIEMAN: Your Honor, my only question is just in terms of the national security presentation, where that would fit into your schedule.

Assuming that the general representations are that the exploit is classified and the information you received in

Michaud, we'd be prepared to go forward in our view. It's clear to me they are not turning over any information about the VEP. I don't know whether you need to make a finding about any of that.

THE COURT: I don't know what the order of things are here. Do we need to have that other hearing before we argue this?

MR. BECKER: Your Honor, as to -- you are speaking as to the ex parte pleading? The question is whether we need to have the ex parte pleading presentation prior to the argument?

THE COURT: Yes.

MR. BECKER: I think, Your Honor, that certainly relates to the motion to exclude. I believe we could proceed on the suppression and the dismissal without that presentation.

THE COURT: All right. We are not going to have a court reporter until 2:30 for that. So let's reconvene at 1:30 and hear argument on the -- first on the motion to dismiss, okay. Then we'll come back on this.

MR. FIEMAN: Did you want also want to hear argument on the suppression issues which are also separate from the ex parte pleading and the discovery issues?

THE COURT: We are going to do these motions one at a time, if that's what you are asking me.

MR. FIEMAN: I just wanted to know if you wanted to

proceed directly to the suppression argument after that initial argument.

THE COURT: We are going to keep plowing until we are done.

MR. FIEMAN: Thank you.

(Luncheon recess.)

THE CLERK: All rise.

THE COURT: Please be seated. Okay, the next matter is the motion to dismiss. I have read all of your submissions on that subject, if I can get them out for reference. I guess the first order of business is argument from the defense. So you may proceed.

MR. FIEMAN: Thank you, Your Honor. I will be relatively brief on this issue because I know it has been thoroughly briefed. There are just a few points that I want to make here. As I will show later, I think there is some overlap with the other issues, because we are looking at really, ultimately, with a lot of this, totality of the circumstances and reasonableness standard. And I understand just how high the bar is legally in terms of dismissing the indictment outright for outrageous conduct, but the circumstances here are unprecedented and deeply troubling, and there are some new facts that were not available to the Court at the time of the Michaud hearing.

I do want to touch about that. We have never, in our

nation's history as far as I can tell, seen a warrant so utterly sweeping. 100,000 potential targets. Something like 8700 IP addresses captured. At least 1152 open investigations. And now oddly enough only, about 214 arrests. And I will be touching on that later.

But what is truly remarkable on top of this is also, of course, the global aspect of it. It is global not only in terms of the jurisdictional Rule 41 issues we are going to be talking about, but global in terms of what the FBI did in terms of disseminating the child pornography.

And I want to be very clear, Your Honor, and that's why -- I found the *Sherman* case a little bit late, and I think it is important because it captures what I have been trying to articulate from the beginning. We are not saying that it's outrageous in any way, shape or form for the government to try and investigate these type of cases on the Tor network. What was outrageous was the way they went about it.

When the *Sherman* court talked about and actually put the government on notice about how it was inexplicable that they would actively distribute, in that case a few videotapes and pictures, in order to investigate their cases, well, it is just vastly more inexplicable in this case and much more disturbing given that prior warning from the Seventh Circuit.

Now, the government has not disputed at this point, I think we are up to now about 62,000 pictures, videos, and

links to pictures and videos that were posted on Playpen. And that's just what's available given the amount of traffic to the site just during the time that the FBI was in control of the site. We put out a conservative estimate of 1 million images downloaded and circulated. There's absolute silence in terms of disputing that from the government, and as I said I think that's a conservative estimate.

So let's just go step back to *Sherman*, and I have some quotes available on the screen, just to show the starting point. In *Sherman*, all the way back in 2001, the Court recognized --

THE COURT: Just a second, I am looking for the citation to *Sherman* here.

MR. FIEMAN: I have it on the screen, Your Honor, 268 F.3d 539. And we filed this in our reply to the government's response to the motion to exclude.

THE COURT: Okay.

MR. FIEMAN: That was a case where the FBI, and I think the postal service or customs had overlapping investigations, and the FBI delivered a catalog of print pictures and VCRs, and some of them actually containing child pornography were sent to the target in the investigation. Just to walk through a few points, and the Seventh Circuit framed this as a warning to the government. It was not raised in the context of a motion to dismiss indictment.

The Court took it upon itself to make these statements, because they were so troubled by it. So first they start "we are aware of the necessity of such tactics" -- in terms of undercover operations and baiting with contraband -- "we are aware of the necessity of such tactics in so-called victimless crimes such as drug offenses, but the use of these methods when victims are actually harmed" -- and they are talking about the children depicted in these images -- "is inexplicable."

And "moreover" -- this is again *Sherman*, continuing with the quote from 549 -- "the government's dissemination of the pornographic materials could hardly be described as a 'controlled' delivery." Well, if it's not a controlled delivery where they were able to send it to the defendant and it sat in his house, I think for a period of time, several weeks, and they recovered it ultimately, the scale of lack of control and heedless distribution in this case is mind boggling.

The Court went on in *Sherman*, "The government's dissemination of child pornography during the investigation resulted in an invasion of privacy of the children depicted. The government here supplied *Sherman* with a literal catalog of child pornography, and then delivered to him materials that depicted actual children, allowing him enough time to view and even copy the materials before arresting him."

And one of the things we've argued is that, and I don't think it's seriously really disputed, is that particularly with the Tor site, there are hosts of things they could have done to maintain the credibility of the site and the traffic to the site without actually distributing child pornography.

And Your Honor, we submitted last week, in response to the latest discovery that were produced by the government, all the things that were going on with the Tor site about how there were problems with the file hosting, the very function that allows you to upload or download. It was slow. Often people couldn't access links. In fact, we know from some of the submissions that we put to the Court, this is actually fairly commonplace with Tor sites because the very rerouting and bouncing around from those that makes it anonymous also makes it slow and often not very functional.

And all of those postings from the undercover agent, who was posing as the administrator, indicate that they were perfectly capable of saying file hosting is down, we are rebooting, we are having access problems. It didn't slow the traffic at all. They could have put out virtual child pornography. They could have put out child erotica.

What's even more disturbing, even if they disagree about the efficacy of some of those methods, we now know from Agent Alfin's recent testimony which we cited, there was absolutely no discussion at the Department of Justice or the FBI about

protocols in terms of handling this stuff or whether these methods of limiting, at least limiting the most egregious distribution were viable. Nobody cared.

This is in face of the warnings that they had from *Sherman*. So again, it's not the fact that they took over a child pornography site. It's not the fact they wanted to keep it up as a criminal undercover site. It's the fact that they simply took no steps, and there's every indication they did not care, that as many as a million or more images were flooding the internet, while they were in total control of the site. I am talking only the time period from the time the FBI rebooted Playpen on its own server and the time they shut it down on March 4th or March 5th. The date is a little unclear.

So that leads me to *Sherman*, as they say on page 550, the Court there said "we have no doubt that creative investigative techniques and tight controls on the materials used as bait for the consumers of child pornography can lead to better protection of the victims of child pornography."

So there, again, they are focussing not on the overarching goal, they are not discounting the difficulties in terms of investigating the type of crime, what they are saying is if you do this, you need to do it extremely carefully and take every possible step to limit the distribution and revictimization.

And we have seen now, we have been asking for information,

getting information for really almost a year now, Your Honor, starting with Michaud, and what we know now is there was no discussion of trying to limit the distribution. There were no protocols for these agents for handling or limiting the distribution of child pornography. And the scale of the distribution now went out to at least 120 countries, at least 1 million images. And it is absolutely mind boggling, we have not seen something like this.

So Your Honor, I started out early on in the *Michaud* case saying I was appalled by this, because with my limited familiarity about the methods and techniques and technology available, I was aware, and certainly my experts, there are lots of ways to go about this when you are not, as the world's largest distributor of child pornography for at least a two-week period, heedlessly and discriminately pumping out and revictimizing children with this type of material.

And Your Honor, I made this analogy before, but what they are doing here is really, I think, fairly simple. Every one of these defendants that I have seen charged in these cases, and I haven't seen all 214, but there's a lot of information that comes my way about other cases, but in every single case that I have seen the person charged is your run of the mill heartland person going to look at some of this stuff, downloading some of it. I don't think -- well certainly these clients have not been charged with distribution, but the

amount of images that are at stake in these cases from the individual clients, and they run in the hundreds, maybe a few thousand, but they are essentially the addicts and couriers who are going to the drug house and the kingpin for this stuff. Whatever justifications the FBI had for stepping into the kingpin role, they should have been darn sure that they weren't distributing pure heroin indiscriminately to the entire world when they were trying to do this. To me that's effectively what happened here.

So Your Honor, I will return to some of these points I think in terms of the probable cause and other issues, but that is essentially our argument. It is not that they took it upon themselves to investigate these crimes, I recognize and I appreciate the difficulties of doing this.

You know, apart from being a defense attorney I am a parent. But as a parent I would want to know that law enforcement, as they are going about with the end in sight of trying to investigate the addicts and the couriers, that they do not themselves step into the role of such a distributor.

Thank you, Your Honor.

THE COURT: Let me ask you a couple questions, and the government may want to comment on some of this. If a user, a Tor user signed into this website and saw child pornography, could that person then download those pictures into his own computer?

MR. FIEMAN: Yes.

THE COURT: Could those pictures then be transferred to others?

MR. FIEMAN: Absolutely, that is routinely what would happen, Your Honor. So let me just follow-up on that point.

One of the very troubling things here, as you know from the NIT warrant, the authorization allowed the FBI to deploy the NIT and complete their searches in a matter of a fraction of a second, at the time the targets landed on the home page. So they had authorization to collect all the information they wanted before anybody actually got the content, and then had the opportunity through this improved file hosting feature the FBI was running, to not only to download, post new images. We know new material, at least 43 series was posted during the time the FBI was running this site, and of course massively redistributed from whatever computers and users had access to it. So that's another aspect of this.

THE COURT: I am not sure I understand that. You mean additional pornography was attached to this site?

MR. FIEMAN: Yes.

THE COURT: By users?

MR. FIEMAN: Yes, Your Honor. The government's disclosure, we submitted their letter, that in addition to all the redistribution, as a result of the FBI maintaining this site, at least 43 new series, new victims were posted --

THE COURT: By Series, you mean --

MR. FIEMAN: For example, you might have 15 or 20 or 100 pictures in a series, or you might have a series of videos, there might be two or three, there might be dozens. And I don't know the exact quantity, because all we know from the disclosure is 43 new series. But during just that window of time that the FBI was running this site, 43 new series. That means things that haven't been seen from the National Center for Missing & Exploited Children were launched onto, uploaded with the assistance of the FBI through their file hosting feature, onto the site, and have now circulated globally and will never be recovered.

And those images are, as you know from the old series we see, they are redistributed endlessly. So the circulation for at least 43 new victims was actively aided and abetted by the FBI.

I have never seen anything like that before, Your Honor. Just to get back to my original point, they didn't have to do that. All the NITs could be deployed from the home page. We'll talk about what that home page showed, the fact that a lot of people could have gone in, said oh my God, this is a child pornography site, and backed out. There's a whole separate series of problems there. But the way they asked for the authorization actually made it completely unnecessary to act -- to distribute any of this stuff.

I can even understand if they saying okay, we are going to narrow this warrant so we are only going to deploy the NIT when people go to specific subdirectories that have a particular kind of content on it, and then once those subdirectories look realistic so will deploy from there, but that's not what they asked. They asked for deployment from the home page.

It was unnecessary and was it heedless, and it was massive.

Thank you, Your Honor.

THE COURT: Okay, thank you. Mr. Hampton.

MR. HAMPTON: Thank you, Your Honor. Again, I want to address two important points that we just concluded on. It is true that over the life of Playpen, not during the two weeks it was under FBI control, but over the life, the FBI and the images and videos they were able to catalog being trafficked in the site, those images contained 42 series. So over that six-month period that had not been seen by anyone, that's true. But that didn't just happen during that two weeks. But that certainly in the end that means there are 42 new series.

Now, we don't know whether that necessarily means new victims or new images and videos that haven't been seen before. All we know is that NCMEC hadn't seen them.

THE COURT: Just a second, if somebody added

something onto this site, doesn't the FBI have it after the site is closed to public access? Can you show me this website now? I don't want to see it, but is it somewhere?

MR. HAMPTON: Your Honor, we do -- there is an off line copy of the website, yes.

The government in its warrant did ask to deploy the NIT at log-in. However, it also made very clear that it may in its discretion choose to deploy it more strategically. That is, deploy it to those who accessed the most egregious content.

So I just want to make clear that the government actually flagged that on the front end that would be a possibility. And in fact that is generally how they approached the operation.

But I think what's important about the defense position, and what they have acknowledged is something, I think, the government on some level doesn't dispute, that these are very tough choices. We are dealing with criminals who are acting with practical impunity, using the anonymity that Tor provides to traffic in the most appalling images and videos that one can think of.

So the law enforcement interests are very strong. But we also have to acknowledge that when the FBI identified this website, identified the opportunity to take it over and to identify -- and then to identify its users through the use of technology, the FBI, the Department of Justice, had to make a

very tough call. Does the potential benefits of identifying those users who are committing horrific crimes with essentially impunity, outweigh the known consequences that that website will continue to be used by those users to trade child pornography?

And the government undertook that balancing before the process was initiated, while Playpen was under FBI control. There were regular meetings. We have discussed those in our pleadings. The FBI asked for a total of 30 days. Ultimately the government concluded to terminate the operation in two weeks.

So the government knew well how tough this choice was. But the legal standard, which I think is what the Court must focus on in evaluating defendants' motion here, is not did the government make a tough choice? Could someone disagree with how the government balanced these interests? The question is did the government act in a way that is so outrageous as to offend fundamental notions of due process and fairness?

Nothing about what the government did was fundamentally unfair to these defendants. These defendants learned about Playpen. They gained access to Tor. They chose to log-in to Playpen and to access it. And they chose to have the collections of child pornography stored on their devices that we found in their homes. The government did not create Playpen. It did not force the defendants to join Playpen or

to download pornography from anywhere. That was the defendant's choice.

And the Ninth Circuit, in applying this outrageous test, the way it determines whether or not the government acted in a way that was so fundamentally unfair, balances these important factors. What was the government's involvement in the crime? The government's involvement was minimal. The government allowed a website that was already in operation to continue to run.

The Ninth Circuit looks to what was the defendant's role in the crime? The defendant's role in the crime was substantial. They are the ones who committed these crimes, not at the urging or behest, not in communicating with the government, but of their own free will.

The Ninth Circuit also looks at the necessity of the technique. And the government explained in detail in its search warrant application and affidavit why this was an appropriate investigative approach. It disclosed that information to the magistrate judge who authorized the warrant, to the district judge who authorized the Title III. And then the government did its very best to minimize the harm.

It monitored the traffic on the site. If it identified individuals that it believed were actively abusing children, it took the steps necessary to try to rescue them. And indeed

some children were rescued and have been rescued since.

And for defense counsel to characterize all the defendants as sort of mere addicts who just accessed a few images, that's not true. There have been cases of producers who were identified. There have been the cases of the individuals who administered this website, who were setting up a system to efficiently transfer huge quantities of child pornography over the internet anonymously.

These are bad people who hurt children. And the government did what it thought was necessary and appropriate, given the technological limitations it faced, to try to identify those people and bring them to justice.

Now, I think it is absolutely fair to say that reasonable people can disagree whether this was the right balancing, whether this is an investigation, an investigative technique that should be used, whether at this point or should it be used in the future. I think that's appropriate. We can have a discussion about that.

But the question is not can someone disagree with what the government did? Can someone conceive of some better way for the government to do it? The question that the government asked so outrageously, that the unfairness of what the government did offends the due process clause and shocks the conscience. And I don't think it can be fairly said that what the government did here was so grossly unfair to the rights of

the defendants, or to anyone as to shock the conscience and to offend fundamental notions of fairness in due process, and I would urge the Court to deny the motion.

THE COURT: What about the statute? 18 U.S.C. 3509(m) that says you have to keep such material in the care, custody and control of the government?

MR. HAMPTON: That's correct, Your Honor, and that's true. But it is well understood that sometimes law enforcement has to do things that would, if not done by law enforcement, be contrary to the law, and so it was a necessary part of this investigation. It is illegal to deal narcotics. The government, however, sometimes in the course of undercover investigations has to allow illegal narcotics to be trafficked. It's the same unfortunate necessity.

THE COURT: There's not the same kind of a statute preventing, arguably preventing what happened here with drugs, is there? That's a different deal. This is a pretty specific statute, you haven't mentioned in your briefing, and I am wondering where it comes in here.

Usually when there's a warrant issued, there's a lawyer somewhere in the background, and I wonder about the ethical propriety of putting this material out to the public in spite of that statute. And I don't know who's making these decisions, but it seems to me it's of concern, both ethically and legally.

MR. HAMPTON: Well, Your Honor, I certainly agree it's a difficult problem. It is not an easy choice for anyone to take on this particular approach, but I think that the way law enforcement works, and has worked from the beginning, has to allow law enforcement the leeway to investigate crimes. That statute certainly -- the statute says what it says. But by necessity, law enforcement has to sometimes do things that if done by someone else might run afoul of the law.

THE COURT: Isn't that basically saying to Congress, I don't care what you think, we are going to do what we think we need to do, to do our jobs.

MR. HAMPTON: Well, Your Honor, I think -- I see how one might read it that way. I don't think that is, though, what -- I don't want to seem flip in responding to statutes, but I think the same argument could be made when the government permits illegal narcotics to be trafficked. Because you are right, while there's not a statute like 3509, it's still illegal for anyone, other than law enforcement, to possess illegal drugs, to possess with intent to distribute, to distribute them. There is that same problem, the government's investigative necessity to prosecute, sometimes to prosecute those crimes, it has to do things that private parties are not allowed to do.

THE COURT: Was this statute even considered by anyone before all this occurred? I don't think we know,

unless Mr. Becker may know.

MR. HAMPTON: Your Honor, Mr. Becker has pointed something out to me, which I apologize should have mentioned at least as to 3509. 3509(m) applies to the discovery context, so it's about discovery in criminal proceedings, so it is narrowly drawn. As to the considerations, without implicating -- it doesn't apply.

THE COURT: Well, the title of the section is Child Victims' and Child Witnesses' Rights, and it has more to do than discovery. But anyway, that's --

MR. HAMPTON: I am referring specifically to subsection (m), which is the section of the statute that relates to the explicit material, the material involved in this case.

THE COURT: Okay.

MR. HAMPTON: One thing I think I should clarify, to make sure that the Court understands what the government is saying here, the government did not at any point create or manufacture child pornography or itself post child pornography. The people who posted and distributed child pornography on Playpen are the users of Playpen. The people who were doing it for months while Playpen was under investigation, and prior to its coming under government control, are the exact same, maybe not identical as there may have been changes in the users, but it's the same set of users

who continued to do that after.

The government simply did not stop Playpen from operating immediately. It allowed it to operate for a brief period so that it could identify those people who were actively sexually exploiting children.

THE COURT: Well, he's going to say you all were doing exactly what the people you just arrested there in charge of the website were doing. So, you know, go ahead with your argument, counsel.

MR. HAMPTON: I understand that is the defense position, but I think it's an important distinction here.

THE COURT: I don't know who wears the white hat, Mr. Hampton.

MR. FIEMAN: Your Honor, just very briefly.

You know, Your Honor, this is the problem with the whole case. First of all, they never disclosed, they never told Magistrate Judge Buchanan that they were going to be operating a child pornography site and redistributing child pornography in the course of this investigation. They never disclosed that on the warrant, and I assure you she never would have signed off on it.

They now say that reasonable minds can differ about what Congress has essentially already decided; this is illegal and you have to maintain custody and control. Again, you know, when they don't like the rules, they don't like Rule 41, they

don't like the Magistrate's Act, they violate their own policies on hacking into foreign countries. Telling, on one hand, the rules committee that we understand Rule 41 does not allow foreign searches, while the whole time they know this is an international search.

They disagree with 3509. They disagree with the statute that you are not supposed to distribute child pornography at all. There was a time we could not even get the mirror image hard copies of our client's hard drives to prepare for trial under the protective orders because they are saying, no, if we hand that to you, we are distributors of child pornography in the context of defending a case pursuant to a protective order. Now they turnaround and tell the Court, well, we didn't post it. Yes, they did post it, because without those file hosting features, none of this could have been done. And if nothing else they kept those up and they improved on it in terms of speed and accessibility.

So reasonable minds can differ except where the law says otherwise, where Congress has said otherwise, where the rules said otherwise. Those decisions have been made.

And we know also, Your Honor, that this warrant was signed off on by an AUSA in Virginia. We don't know what debate was going on except from October 11th, Agent Alfin's testimony that this was debated by high levels in the FBI and DOJ. And yet they elected, either the FBI on its own, and we've

certainly seen the FBI willing to go out on a limb by itself regardless of the advice of DOJ on a number of occasions or whether nobody simply cared.

And this is really the crux of it. The ends are okay. The means were deplorable. It's reassuring that they did not produce child pornography. If that's what we're reduced to, that's great.

But the problem here, Your Honor, is that while trying to solve one problem and avoid revictimization of some children, they created a massive new one. And we have seen no protocols, no explanation for why they did it this way.

Every one of those people who's been arrested was arrested based on IP information that was collected at the point that they landed onto the home page. Everything after that was completely unnecessary.

Your Honor, to the extent that reasonable minds can differ about this, and I don't think they can, particularly given the warning, the explicit warning that was in the *Sherman* case, and the fact that this was never disclosed to Magistrate Judge Buchanan in terms of how this investigation was going to be done, I am asking the Court to make a referral to the Department of Justice and the FBI, Offices of Inspector General.

To whatever extent that there are reasonable differences that can be elucidated, to whatever extent the attorneys

involved in this and the Department of Justice and in Virginia and the FBI did not take proper precautions in the handling or distribution of child pornography may have violated their bar oaths, I think all this needs to be sorted out, not just based on the limited information that we have, but internally as well.

If they don't want to disclose their deliberations, and the Court has already ruled on that, we respect that ruling although we object to it, then let them do it in-house. Let's have the IG offices do that in an appropriate manner and make recommendations about this.

But at this point we only know what happened in the end, it was not disclosed to the magistrate, at least a million images out there, and absolutely no investigatory need to do this.

Thank you, Your Honor.

THE COURT: Thank you. Now, are you prepared for this other hearing at this point, Mr. Becker?

MR. BECKER: For the ex parte matter, Your Honor?

THE COURT: Yes.

MR. BECKER: Yes, Your Honor, we have the documents available.

THE COURT: Okay, I see our court reporter in the back, too. Why don't you all get set up and we'll do that next and then come back to court --

MR. BECKER: Very well, Your Honor.
THE COURT: -- and finish the rest of this.
Let Dara know when we are ready. Just give me a minute, I want to read the motion and the reply again before we start. Okay.
MR. BECKER: Very well, Your Honor.
THE COURT: You all ready?
MR. BECKER: Yes.
THE COURT: Okay, well give me a couple minutes to read this.
MR. BECKER: Thank you, Your Honor.
THE COURT: Again.
(Recess taken.)
THE COURT: Okay, I will give you a short ruling after I take ten minutes or so. We'll reconvene about 3:15.
(Recess taken.)
THE CLERK: All rise, Court is again in session.
THE COURT: Please be seated. Okay, first I should give you a ruling on the ex parte and in-camera hearing that we just completed. The real subject was three areas of discovery that the plaintiffs have made. It is my judgment that the discovery need not be disclosed by the government based on what I learned and heard at the in-camera ex parte hearing.
Other issues remain, as do whether that material is

relevant and helpful and material to plaintiffs and whether a summary can or should be substituted. I don't reach those issues.

Now, the remaining matter today is the third motion, which is the motion to suppress. I know it's Halloween and I know some of you probably can't wait to go trick or treating. I am good for the day, but I don't know what issues you have. I want to give you plenty of time to argue this last motion which has a lot of parts to it. But you tell me when you want to stop.

MR. FIEMAN: Well, Your Honor, if I may approach. First of all, just to clarify where we are in terms of discovery issues. If I understand, the Court has determined that, as it did in Michaud, that the government need not turn over the components. We would still like to argue, however, which is essentially the same on Michaud, the sanctions that should imposed for nondisclosure. I don't know if you want to hear argument on that, I was a little unclear, because we believe we are in the same position that we were in the prior case.

We do have argument about -- it's the same situation that we talked about from *Jencks* and everything. The government clearly has classified information, and they have a right not to hold it --

THE COURT: Wait, I want to give you time to argue

whatever it is you want to argue. The question before the house is how long you want to argue this afternoon?

MR. FIEMAN: Well, I know that Mr. Hamoudi's son is hoping he'll be home around 5:00 to go trick or treating. I may have about 45 minutes or an hour of argument.

My request, and I think it's joined, is that we reconvene tomorrow morning for the remaining issues. We've done all the evidence. It shouldn't take much -- it will take the morning, at most.

THE COURT: You are telling me you don't think we'll be finished tonight anyway?

MR. FIEMAN: No, Your Honor, not with both arguments, and I know counsel have points they want to make apart from my general arguments.

THE COURT: Mr. Becker, you are hiding behind that machine. I don't know if you are making nasty faces at me or what.

MR. BECKER: Definitely not, Your Honor.

MR. HAMPTON: Your Honor, we'll defer to the Court. We are happy to come back tomorrow morning and finish things up, that's fine.

THE COURT: Well, that's fine with me, I guess. It doesn't matter to me a lot one way or the other. I hate to lose an hour, but I have got tomorrow entirely clear.

I intended to start out this morning by telling you that I

have made a bad mistake in this case in authorizing over-length briefs. I read all your briefs, most of it twice, on these three motions. And they all could have been done within the time limits very nicely and they would have been better briefs. I guess what I am leading up to is I feel the same about argument here. Try and keep it succinct and to the point and bear in mind I have read your briefs.

MR. FIEMAN: I will use the evening to edit my notes, Your Honor.

THE COURT: That would be good.

Okay, well, we'll reconvene tomorrow at 9:30, then, and finish the argument in this case. And happy Halloween.

(The Court recessed to Tuesday, November 1, 2016, at the hour of 9:30 a.m.)

* * * * *

C E R T I F I C A T E

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/S/ Teri Hendrix _____ November 21, 2016

Teri Hendrix, Court Reporter Date